A Quarterly Journal Devoted to All Aspects of Cryptology

CRYPTOLOGIA

Volume 8 Number 3 July 1984

CRYPTOLOGIA A Quarterly Journal Devoted to All Aspects of Cryptology

All correspondence concerning subscriptions, advertising and publications should be sent to the publisher at the Editorial Office, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803. TELEX 752486.

See inside back cover for subscription information.

ISSN 0161 - 1194. Manufactured in the United States of America.

Cover: A source for Naval intelligence? See first article.

Assistance of Rose-Hulman Institute of Technology is acknowledged and appreciated.

THE ORIGINS OF RUSSIAN NAVY COMMUNICATIONS INTELLIGENCE

Translated by Thomas R. Hammant

[Editor's Note: The article is reprinted from the May 1976 issue of Cryptolog, a publication of the Naval Cryptologic Veterans' Association.

It shows with much concrete detail the accidental nature of the beginnings of COMINT in the Russian navy — the same unplanned basis that it had in the British and German navies and in the German army, at least, as well. Unfortunately, it does not clear up a discrepancy about the German codebook that the Russians gave the British. Winston Churchill in The World Crisis claimed, rather dramatically, that the Russians found it with the body of a drowned German under-officer "clasped in his bosom by arms rigid in death." But Patrick Beesly, in his Room 40, says that the German codebook now in the Room 40 records in the Public Record Office shows no sign of immersion. This account further complicates the matter by stating that the codebook was photographed and the pictures given to the British. Perhaps further research will clarify this.]

[Translator's note: The following article is a translation of "On the Origins of Communications Intelligence in the Russian Navy," by V. Yankovich, in the Soviet periodical Voenno-Istoricheskij Zhurnal (Journal of Military History), February 1961, pp. 114-117. In my search of open-source materials, Yankovich's article was the only one that I could find that describes the early development of the Soviet signal intelligence service from the point of view of a participant. The article does not contain any attribution as to the source of the information, or any identification of the author except his statment in the article that he was a "staff flag officer" there at the time. Because of the article's unique nature and its interest to readers, I have translated it in its entirety.]

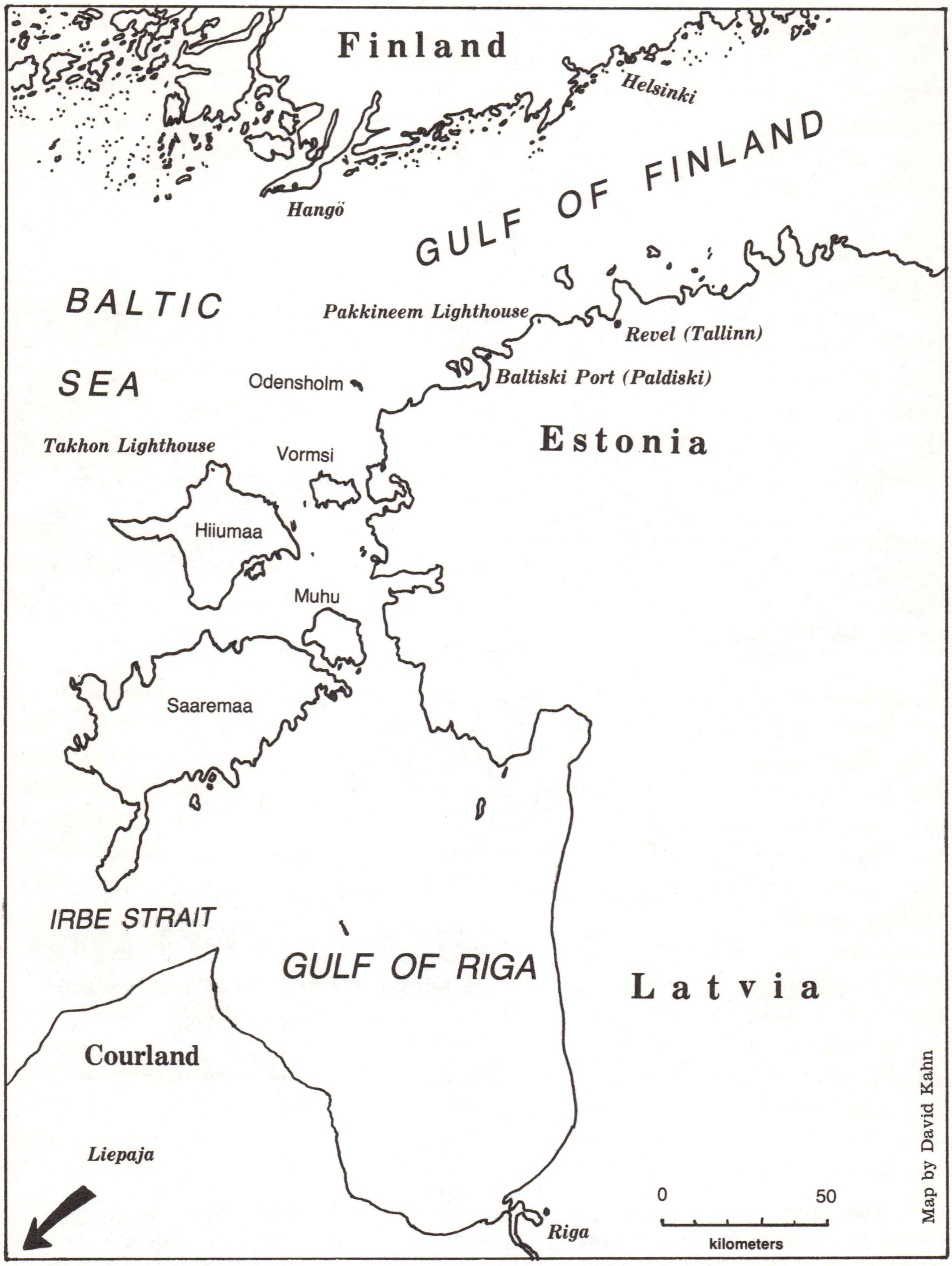
[Author' note: It should be noted that the descriptions accompanying the charts in Morskoj Atlas (Naval Atlas) (Vol. 3, Part I, Publishing House of the Main Staff of the Navy, 1959, p. 769) and in Istoriya Voenno-Morskogo Iskusstva (History of the Naval Art) (Vol. 3, Moscow, Voenizdat, 1953, p. 120) are not completely accurate in illuminating the circumstances under which the documents were found on the German cruiser Magdeburg, or about the contents.]

At the beginning of World War I not one of the combatant sides had a specially organized communications intelligence (COMINT) service [radiorazvedka] in its navy. The first steps toward organizing a COMINT effort in the Russian Navy were, to a large degree, connected with the wreck of the German cruiser Magdeburg near Odensholm Island on 26 August 1914. Documents discovered on that ship revealed a system of enciphered radio communications that the enemy had been using at that time.

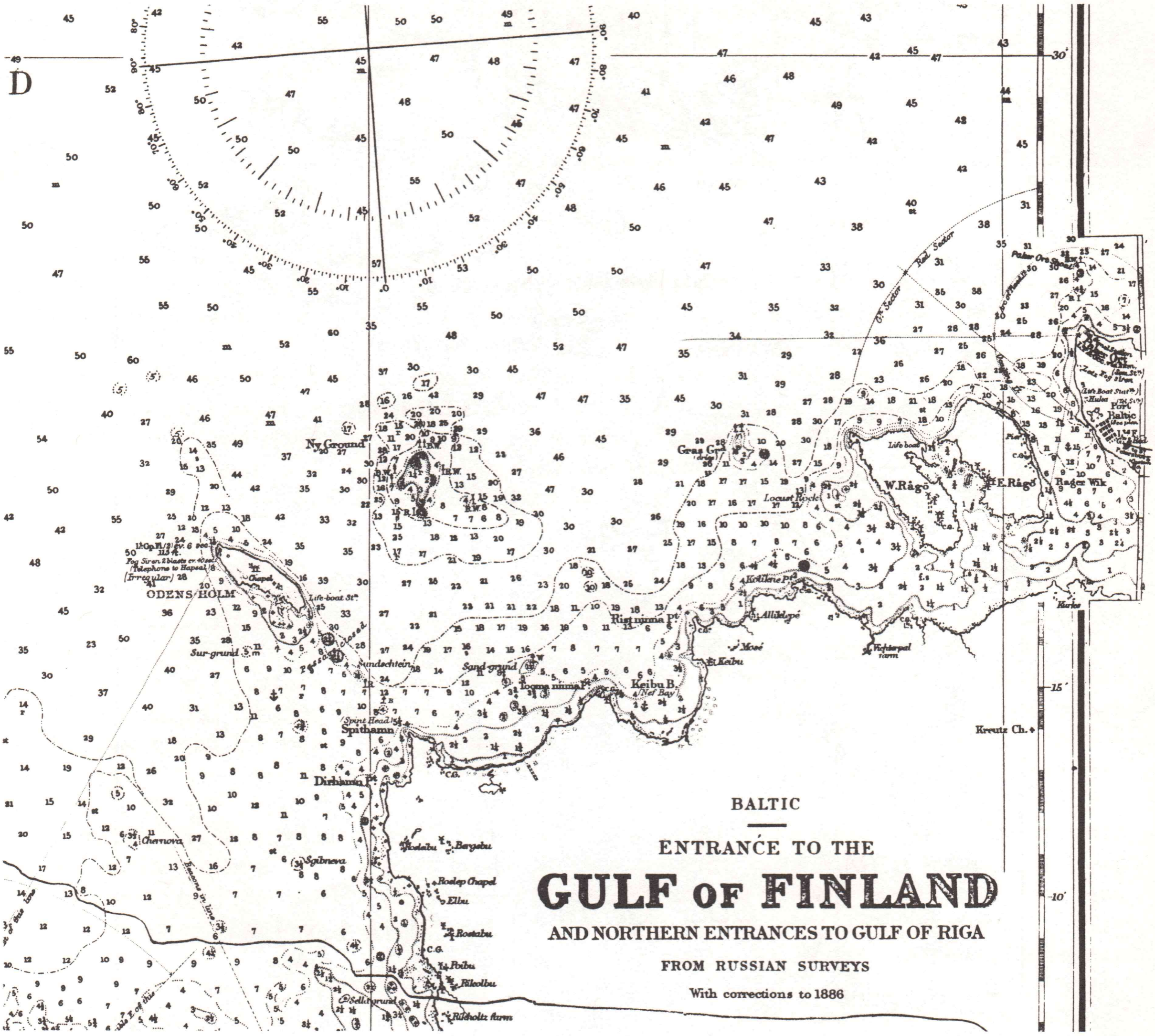
After Germany declared war on Russia on 1 August, the enemy fleet in the Baltic Sea limited itself for a prolonged period of time to demonstrations carried out by small forces and the patrol service in areas of possible Russian naval action

In the early hours of 26 August the Russian patrol cruisers Pallada and Bogatyr' were standing at anchor in Baltiski Port (now Paldiski) because of fog. At 0130 hours the signal station on Odensholm (now Osmussar) Island reported by telephone to the chief of the signal service in Revel (now Tallin) that a ship had run aground at a distance of two cable lengths from the island. Then the signalmen reported that they could hear German being spoken and the operation of shipboard machinery, and could also hear the anchors being veered and heavy objects being thrown overboard. When the fog lifted somewhat, the signal station reported that a four-funneled cruiser had run aground and that a torpedo boat was standing by it, attempting to tow the cruiser by the stern. Upon receiving the very first report in Revel concerning the accident that had befallen the German ship, the fleet commander dispatched the First Torpedo Boat Division and the cruisers Bogatyr' and Pallada to Odensholm Island. The chief of the fleet communications service set out to sea from Revel on board the torpedo boat Lejtenant Burakov, accompanied by the torpedo boat R'yanyj; they were followed somewhat later by the cruisers Rossiya and Oleg, and finally, the Ryurik, under the flag of the fleet commander.

The cruisers Bogatyr' and Pallada approached Odensholm in the fog and, at approximately 1100 hours, when the visibility had temporarily improved, they spotted the German cruiser Magdeburg aground, with a tow line from the large



Where the Magdeburg Grounded
The German cruiser ran aground off Odensholm, now called Osmussaar. This is at the entrance to the Gulf of Finland. In 1914, the Baltic islands belonged to the Russian Empire, as did Finland, Estonia, and Latvia.



Odensholm
This detail from a contemporary Admiralty chart, No. 2241, corrected to May 1980, shows the three-mile-long island at 59 degrees 18 minutes north latitude, 24 degrees 27 minutes east longitude, about five miles off Spint Head, the northwestern point of Estonia. On the island's seaward (northwestern) tip is a lighthouse, equipped with a fog siren giving 2 blasts every 40 seconds, off which the Magdeburg grounded. Ny Ground, to the northeast, is a sandbar.

German torpedo boat, the V-26, attached to its stern. Our cruisers opened fire on them. The Magdeburg responded, but its situation was hopeless, and, as was subsequently reported by captured German sailors, the commander decided to blow up the cruiser. The V-26 was ordered to approach the Magdeburg and take off the crew. However, it failed to throw out the mooring lines. Taking advantage of the dense fog, the torpedo boat left. After it departed, the forward magazines of the Magdeburg were exploded.

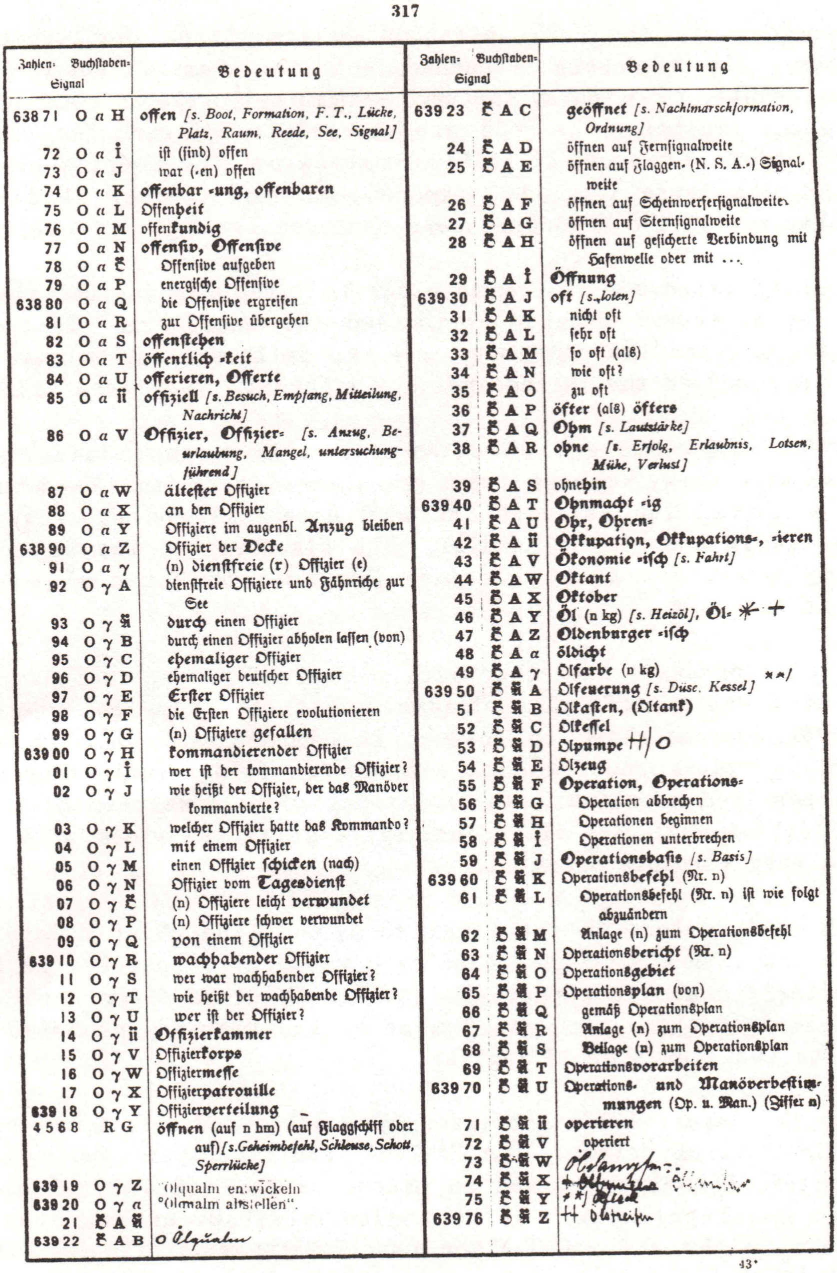
When visibility improved, it became clear that the Germans had abandoned the cruiser. The Lejtenant Burakov approached the Magdeburg. The only people remaining on it were the commander and two sailors. Approximately 50 crew members were found on the island and in a lifeboat. They were taken prisoner.

A large number of bundles and suitcases containing personal articles belonging to the cruiser's crew members were transferred from the Magdeburg to the Lejtenant Burakov. The articles included notebooks and diaries. A signal book was found in one of the bundles. The discovery of the signal book was reported by semaphore to the cruiser Ryurik, which had also approached Odensholm at that time.

The fleet chief of staff, together with several officers, including myself -- at that time I was a staff flag officer — set off from the Ryurik on board the destroyer Pogrannichnik to inspect the Magdeburg. When inspecting the radio room, I noticed under a desk a cardboard folder containing a piece of paper with penciled notations. The notations might have been of interest, so I took the folder with me. That insignificant little piece of paper turned out to be a very valuable document.

Upon the Ryurik's return to the Revel roadstead, the chief of staff ordered me, as a person with a good knowledge of German, to acquaint myself with the captured materials and to report the results to him. After setting down to work, I noticed that the authors of most of the diaries and notebooks dwelt especially on the events of 17 August.

On that day (17 August 1914) a brigade of Russian cruisers consisting of the Gromoboy, the Admiral Makarov, the Pallada, and the Bayan, under the command of Rear Admiral Kolomejtsev, was on patrol on the meridian of the Pakerort (now Pakkineem) lighthouse. At approximately 1500 hours, our observers noticed smoke to the west of Takhkon (now Takhkuna) lighthouse. The brigade started out in that direction and quickly spotted two German cruisers, which were drawing closer to the Russian cruisers. Flagship navigator Sakelari expressed the hypothesis that the enemy was intending to lure the brigade into a minefield. Admiral Kolomejtsev agreed with his navigator and ordered the brigade to turn back to the east.



317

Zahlen=	Buchſtaben=	Bedeutung
Signal		
63871	O α H	**offen** *[s. Boot, Formation, F. T., Lücke, Platz, Raum, Reede, See, Signal]*
72	O α İ	iſt (ſind) offen
73	O α J	war (=en) offen
74	O α K	**offenbar =ung, offenbaren**
75	O α L	Offen**heit**
76	O α M	offen**kundig**
77	O α N	**offenſiv, Offenſive**
78	O α Ö	Offenſive aufgeben
79	O α P	energiſche Offenſive
63880	O α Q	die Offenſive ergreifen
81	O α R	zur Offenſive übergehen
82	O α S	**offenſtehen**
83	O α T	**öffentlich =keit**
84	O α U	**offerieren, Offerte**
85	O α Ü	**offiziell** *[s. Besuch, Empfang, Mitteilung, Nachricht]*
86	O α V	**Offizier, Offizier=** *[s. Anzug, Beurlaubung, Mangel, untersuchungführend]*
87	O α W	**älteſter** Offizier
88	O α X	**an** den Offizier
89	O α Y	Offiziere im augenbl. **Anzug** bleiben
63890	O α Z	Offizier der **Decke**
91	O α γ	(n) **dienſtfreie (r)** Offizier (e)
92	O γ A	dienſtfreie Offiziere und Fähnriche zur See
93	O γ Ä	**durch** einen Offizier
94	O γ B	durch einen Offizier abholen laſſen (von)
95	O γ C	**ehemaliger** Offizier
96	O γ D	ehemaliger deutſcher Offizier
97	O γ E	**Erſter** Offizier
98	O γ F	die Erſten Offiziere evolutionieren
99	O γ G	(n) Offiziere **gefallen**
63900	O γ H	**kommandierender** Offizier
01	O γ İ	wer iſt der kommandierende Offizier?
02	O γ J	wie heißt der Offizier, der das Manöver kommandierte?
03	O γ K	welcher Offizier hatte das Kommando?
04	O γ L	**mit** eimem Offizier
05	O γ M	einen Offizier **ſchicken** (nach)
06	O γ N	Offizier vom **Tagesdienſt**
07	O γ Ö	(n) Offiziere leicht **verwundet**
08	O γ P	(n) Offiziere ſchwer verwundet
09	O γ Q	**von** einem Offizier
63910	O γ R	**wachhabender** Offizier
11	O γ S	wer war wachhabender Offizier?
12	O γ T	wie heißt der wachhabende Offizier?
13	O γ U	**wer** iſt der Offizier?
14	O γ Ü	**Offizierkammer**
15	O γ V	Offizier**korps**
16	O γ W	Offizier**meſſe**
17	O γ X	Offizier**patrouille**
63918	O γ Y	Offizier**verteilung**
4568	R G	**öffnen** (auf n hm) (auf Flaggſchiff oder auf) *[s. Geheimbefehl, Schleuse, Schott, Sperrlücke]*
63919	O γ Z	"Ölqualm entwickeln
63920	O γ α	°Ölqualm abstellen".
21	Ö A Ä	
63922	Ö A B	o Ölqualm
63923	Ö A C	**geöffnet** *[s. Nachtmarschformation, Ordnung]*
24	Ö A D	öffnen auf Fernſignalweite
25	Ö A E	öffnen auf Flaggen= (N. S. A.=) Signalweite
26	Ö A F	öffnen auf Scheinwerferſignalweite
27	Ö A G	öffnen auf Sternſignalweite
28	Ö A H	öffnen auf geſicherte Verbindung mit Hafenwelle oder mit ...
29	Ö A İ	**Öffnung**
63930	Ö A J	**oft** *[s. loten]*
31	Ö A K	nicht oft
32	Ö A L	ſehr oft
33	Ö A M	ſo oft (als)
34	Ö A N	wie oft?
35	Ö A O	zu oft
36	Ö A P	**öfter** (als) **öfters**
37	Ö A Q	**Ohm** *[s. Lautstärke]*
38	Ö A R	**ohne** *[s. Erfolg, Erlaubnis, Lotsen, Mühe, Verlust]*
39	Ö A S	ohne**hin**
63940	Ö A T	**Ohnmacht =ig**
41	Ö A U	**Ohr, Ohren=**
42	Ö A Ü	**Okkupation, Okkupations=, =ieren**
43	Ö A V	**Ökonomie =iſch** *[s. Fahrt]*
44	Ö A W	**Oktant**
45	Ö A X	**Oktober**
46	Ö A Y	**Öl** (n kg) *[s. Heizöl]*, **Öl=** * +
47	Ö A Z	**Oldenburger =iſch**
48	Ö A α	**öldicht**
49	Ö A γ	Öl**farbe** (n kg) **/
63950	Ö Ä A	Öl**feuerung** *[s. Düse, Kessel]*
51	Ö Ä B	Öl**kaſten, (Öltank)**
52	Ö Ä C	Öl**keſſel**
53	Ö Ä D	Öl**pumpe** H/O
54	Ö Ä E	Öl**zeug**
55	Ö Ä F	**Operation, Operations=**
56	Ö Ä G	Operation abbrechen
57	Ö Ä H	Operationen beginnen
58	Ö Ä İ	Operationen unterbrechen
59	Ö Ä J	**Operationsbaſis** *[s. Basis]*
63960	Ö Ä K	Operations**befehl** (Nr. n)
61	Ö Ä L	Operationsbefehl (Nr. n) iſt wie folgt abzuändern
62	Ö Ä M	Anlage (n) zum Operationsbefehl
63	Ö Ä N	Operations**bericht** (Nr. n)
64	Ö Ä O	Operations**gebiet**
65	Ö Ä P	Operations**plan** (von)
66	Ö Ä Q	gemäß Operationsplan
67	Ö Ä R	Anlage (n) zum Operationsplan
68	Ö Ä S	Beilage (n) zum Operationsplan
69	Ö Ä T	Operations**vorarbeiten**
63970	Ö Ä U	Operations= **und Manöverbeſtimmungen** (Op. u. Man.) (Ziffer n)
71	Ö Ä Ü	**operieren**
72	Ö Ä V	operiert
73	Ö Ä W	[illegible]
74	Ö Ä X	+ ~~[illegible]~~ [illegible]
75	Ö Ä Y	**/ Ölfleck
63976	Ö Ä Z	++ Ölstreifen

43*

A page of the Signalbuch der Kaiserlichen Marine (Berlin, 1913) - the codebook of the German navy. A copy of this code was recovered by the Russians from the Magdeburg and given to the British.

By comparing the entries, I managed to ascertain that the cruisers Augsburg and Magdeburg and three torpedo boats had the mission of convoying the minelayer Deutschland, with 800 mines, to the mouth of the Gulf of Finland. The cruisers were proceeding ahead, followed at a slight distance by the minelayer and the torpedo boats. As the Germans were already approaching the designated place for the laying of the minefield, they saw that a brigade of Russian cruisers that was stronger in armament was coming toward them. The German admiral on the Augsburg ordered the Deutschland to depart to the west at full speed. He had decided to join battle with the Russian ships in order to attract them to his own ship, to gain time, and thus to save the minelayer. The German cruisers could always disengage from combat because of their great advantage in speed. And so, when our brigade, unexpectedly for the enemy, avoided contact, the tense situation for the Germans was replaced by one of elation. The Deutschland immediately returned, and the German admiral reported to his command the satisfactory completion of the operation.

In view of their avoidance of combat, in which it might have been possible to destroy the German cruisers, or, pursuing them in battle, to overtake the very slow-moving Deutschland, Rear Admiral Kolomejtsev and navigator Sakelari were removed from active duty.

But what were the coordinates of the mine obstacle that had been laid by the Germans? The answer to that question was obtained after a study of the piece of paper that I had taken from the radio room. The initial designations that were customary for all radiograms were followed by text consisting of combinations of letters. That prompted me to turn to the signal book. The deciphered top secret enemy report stated that a minefield had been laid at such-and-such a time on 17 August, and indicated its exact coordinates in our waters.

The Fleet Staff immediately reported this information to everyone with a need to know. Our minesweepers checked the position of the minefield and subsequently that field was the first link in a large advance mine position that we gradually created across the Gulf of Finland. During the war many enemy ships found a grave there.

Finding the connection between the German radiogram on the laying of the minefield and the signal book had the most important and far-reaching consequences. It made it possible for the Russian and Allied naval command elements to use the intercepted enemy radio transmissions for intelligence purposes. The COMINT service that we organized consisted, first, in receiving and solving the enemy's enciphered radiograms, and second, in providing bearings on operating German shipboard radio sets, as obtained by our shore-based radio stations.

A subsequent check of intercepted German radiograms confirmed that the enemy was enciphering his conversations by a combination of literal and digital characters in the signal book. Participating in the exploitation of this material, in addition to Flagship Radio Specialist I.I. Rengarten and myself, were two other persons — an additional officer and an enlisted-rank radiotelegraph operator -- who were assigned specifically for permanent work in COMINT. It was assumed that the Germans might subsequently change their system of encipherment.

That question was carefully thought out at the Fleet Staff, and the fleet commander, jointly with the chief of the communications service, decided to organize urgently a special-purpose radio-interception [priemnaya] station in the western part of the southern shore of the Gulf of Finland. To achieve better monitoring of the ether, the site chosen was in the woods, far from populated areas. All the buildings were hidden from outside view and the station's personnel were allowed no contact with the outside world. The necessary supplies were delivered to the station at specified times by car from Revel. The radio station was tasked with only listening to German radiograms on several radio receivers. An underground cable connected the radio station with the southern region administration of the signal service. The station's personnel were carefully selected from the officers and the best radiotelegraph operators who knew German. The work of the stations was kept in strict secrecy to prevent the enemy from learning of its existence. Even in the Russian Navy only a few people knew about it.

The Germans used radio communications widely, and soon our special-purpose radio station had accumulated extensive material on various aspects of life, service, and combat actions of the German Fleet.

COMINT helped to keep the command of the Baltic fleet well informed on the enemy and made it possible for the fleet, within a short period of time, to change over from the passive waiting for the German fleet to appear in the Gulf of Finland to active operations in the southern part of the Baltic Sea.

After a short period of time the enemy, assuming the possibility that his radiograms were being intercepted, decided to make the cipher more complex. For that purpose he began to make it a practice to take the text that had been enciphered according to the signal book and then re-encipher it with the aid of re-encipherment tables [pereshifrovochnye tablitsy]. The tables were changed from time to time. However, that circumstance did not present much of a problem in deciphering the German radiograms. By that time the workers at the radio station had collected extensive material on the basis of the deciphered radiograms. They needed only a few hours to figure out the new re-encipherment chart.

Soon our divers found a second signal book at the bottom of the sea in the area where the Magdeburg had been. At Fleet General Headquarters the book was photographed, and copies were supplied to our Allies, the British and the French.

The Naval Commission for Investigation and Utilization of the Experience Gained by the 1914-1918 War at Sea noted that our COMINT service had achieved great success for several months of the war.

It was interesting for me and the other naval specialists who participated in breaking the system by which the enemy enciphered his radiograms to follow the subsequent development of that work.

The biggest achievement was the ability to use the available materials to create the most commonly used parts of the new signal book after the Germans withdrew from use the old signal book which we had. After receiving the signal book from us, the British also organized a COMINT effort, carrying out similar work in studying German radiograms.

The enemy made wide use of his radio communications. His stations operated constantly. Naval Staff Officer Captain 2nd Class I.I. Rengarten suggested installing at our coastal radio stations the very simple radio direction finders that he had invented as early as 1912. Following successful testing, the devices were installed at many coastal observation posts where there were radio stations. It was possible to determine the enemy's whereabouts by receiving radio bearings at two points simultaneously.

The time came when the chief of the signal service began to bring the Fleet Staff a map of the Baltic Sea on which various colors of ink were used to designate the routes taken by enemy ships. Therefore it is not by accident that the Russian ships avoided the German minefields and remained undetected when setting up our own minefields near the German shores.

The command element of the Baltic Fleet made wide use of the COMINT information. The following are a few examples.

The German Naval Staff established a course for their ships to follow when entering or leaving the Gulf of Danzig. On 14 February 1915, two of our torpedo boats laid mines on that course. The very next day COMINT reported that a German transport had been blown up.

We also learned the arrival time of a German cruiser at the port of Libau (now Liepaya) and its departure time. A submarine was sent to the entrance to the port. As the German cruiser was leaving Libau, it was sunk by that submarine.

Following the occupation of Courland (West Latvia) by the German troops, the German Ground Forces Command, which was rushing to seize Riga, requested the Naval Staff to provide support from the sea. COMINT revealed these conversations and established the date of the planned operation. The [Russian] fleet commander decided to strengthen the naval forces in the Gulf of Riga by sending the battleship Slava. On 31 July 1915 the Slava took the enemy completely by surprise by crossing over from the Gulf of Finland to the Gulf of Riga. COMINT provided such good information about the enemy's plans that when the German fleet, on the morning of 8 August, approached Irbe Strait, our torpedo boats and two gunboats were already waiting for them. By 1000 hours the Slava also approached the strait. The Germans' plan to break through into the Gulf of Riga was thwarted.

Early in November 1916, COMINT reported that the enemy was preparing an operation in the southern part of the Gulf of Finland. Information received permitted the hypothesis that a raid by torpedo boats on Baltiski Port was expected. The Fleet Staff felt that the Germans would know of the existence of an open passage in the southern part of the forward mine position. The fleet commander ordered the laying of mines immediately in that passage. During the night of 10-11 November, our radio stations intercepted fragments of conversations between enemy torpedo boats that had suffered a calamity. Two of them had been blown up in the minefields that we had just laid. Then everything became quiet. After approximately an hour and a half, the German torpedo boats began firing on Baltiski Port. At approximately an hour after that, eight German torpedo boats that were returning to the west came upon the minefield. The flotilla moved along the minefield and then turned to the west again. The torpedo boats began to blow up. During the course of an hour, five of the eight torpedo boats were sunk. All told, seven out of 11 of the newest torpedo boats were sunk.

Thus, by making skillful use of COMINT information, Russian sailors of the Baltic Fleet were, throughout the war, completely aware of the intentions of the enemy's naval forces.

A CRYPTOGRAPHER'S WAR MEMORIES

FRANCIS GUELKER

Some 40 years have passed since my World War II experience as a cryptographer with the 50th Signal Battalion of the VII Corps, commanded by General J. Lawton (Lightnin' Joe) Collins, but some memories never fade away, and perhaps a few of my reminiscences might be of some interest.

Born in St. Louis, Missouri, in 1922, and a lifelong resident of that "Gateway to the West," I was, from childhood, interested in word puzzles, anagrams, and mathematical teasers. So, as my educational pattern emerged, I naturally was drawn to courses that stimulated that interest.

While attending Harris Teachers College in St. Louis, I heard from a classmate that the U.S. Army was accepting volunteers for training in the U.S. Signal Corps, and I decided to enlist as a "civilian trainee" in the so-called Enlisted Reserve Corps. I was promptly assigned to a local technical school, Hadley Technical. Entrance screening tests evidently convinced the examiners that my training should be in the areas of mathematics, typing, basic radio theory, and related subjects. I was fortunate that these test results corresponded with my inclinations. However, prior to acceptance in the ERC, my background, friendships, and habits were closely investigated by the FBI, causing some eyebrow-raising by neighbors and friends, who wondered what I had been up to!

Together with about 12 other ERC civilian trainees, we spent some 6 months at Hadley Technical School studying these subjects. At this time, we had no indication of our eventual Army assignments, nor did we receive any training in basic cryptology during this period.

Our small ERC group was then inducted into the U.S. Army and received additional training at Camp Crowder, near Joplin, in southwest Missouri. This included such subsequently unused training as telephone pole climbing; since we were a Signal Corps group, this was de rigueur for all. We wore sharp pole-climbing spikes and one trainee, after almost reaching the top of the 30-foot slippery pole, missed his footing and fell the length of the pole — his safety belt slamming him into the pole several times as he fell -- and at the bottom the spike from one boot penetrated the instep of the other foot, causing a severe, bloody wound. The sergeant in command yelled, "Who told that man to come down?" — and made him climb back up until he rested his chin at the top of the pole, as originally ordered!

Frank T. Guelker

After basic training was completed, we were transferred to Fort Monmouth, New Jersey, where we received intensive cryptographic training. The classes at Fort Monmouth were larger — perhaps 40 or 50 — and certainly many more than modern educators consider "optimum class size!" During my stay, there were at least 5 or 6 such classes under way at the same time. However, the instructors were exceptionally good, and I feel that we received excellent training in fundamental cryptography — enciphering and deciphering, frequency tables, polyalphabetic systems, double transposition ciphers, and similar basic instruction.

The training was rigorous, with much study after class, so that for several months we hardly had time to leave this sprawling, uninteresting camp. This concentration of effort resulted in perhaps a 50% reduction in class size.

After completion of this training, some 10 or 12 of us were formed into a temporary group and crossed the Atlantic on the packed-to-the-scuppers old ship Ile de France, landing at the port of Greenock/Gourock, Scotland, in the firth of the river Clyde. With little delay at Glasgow, about half of our small group was transported to Bletchley Park, in Buckinghamshire, England, where was located the Government Code and Cypher School, Britain's cryptologic agency. It was on a sizable estate with a red-brick late-Victorian country house and a number of Nissen huts. Here we received concentrated Top Secret cryptographic training. The wooden Nissen huts were similar to the present-day "Butler Buildings" and were "bloody cold and damp." We only stayed several weeks.

The cross-channel invasion being imminent, we took our place in the massive troop movements from all parts of England to the south coast, embarking in early June, 1944, in an LCT (landing craft, tank). We were part of VII Corps.

My unit landed on 12 June (D-day + 6, as it was later designated), after a relatively secure position had already been established on the beach. We immediately set up a temporary cryptographic station under a camouflage tarpaulin spread in the overhanging trees. Initially, we utilized the M-209 cipher machine strapped to our thigh above the knee. This machine had a "Confidential" security rating only, but within a few days, our Sigaba equipment was brought ashore, mounted in a covered 2 1/2 ton truck.

Needless to say, the conditions in France at that time were quite different from the comparatively tranquil atmosphere at Bletchley Park. But, the noise, danger, and hectic activity all around certainly tended to "concentrate the mind wonderfully," as Samuel Johnson once wrote of a man facing death.

In the Cherbourg campaign alone, over 39,000 prisoners were taken by the VII Corps, against the cost of 2800 Americans killed, 13,500 wounded, and 5,700 captured or missing.

The drive inland took the VII Corps south out of Normandy, through St. Lo, Mortain, Mayenne, Chartres, Melun (south of Paris), into Belgium at Mons, through Leige, and then into Germany at Aachen, through the districts around Cologne, Marburg, Paderborn, and Nordhausen, for junction with the USSR forces at Leipzig, Germany on 30 April 1945.

This total drive from 6 June 1944 to 30 April 1945 comprised a distance of only about 1300 miles, but, of course, to us it seemed like 13,000! Although this effort included many "troublesome" periods (such as the Breakthrough at St. Lo, the Battle of the Bulge, the Rose Pocket, and others), after four decades, memories more frequently revolve around the relatively inconsequential, and, in hindsight, more amusing occurrences.

Such as the piping-hot pommes frites prepared by a group of nuns in the area of Liege, Belgium, and served to us in abundance and joy as we approached their convent -- I can still taste them!

Or, how several of us were rummaging one night in the dark inside a large private home in a bombed-out section of Cologne, when the elderly German owner suddenly appeared behind us and quietly said "Also?", causing us to whirl about and realize how easily we could have been wiped out because of our carelessness.

From a security standpoint also, one incident often recurs to mind, in which, fortunately, I was not a participant. Upon entering Aachen, Germany, corps headquarters had to stay put in a large government building for several days to permit support groups to catch up with us. To avoid enemy detection from the air, we parked the 2 1/2 ton covered truck that contained our Sigaba and other equipment underneath a massive archway leading from the front drive to the rear courtyard. Security instructions were that this truck was never to be left unattended. That night, around midnight, two cryptographers were on duty in the truck. One soldier left the truck to answer a "call of nature." While he was gone, the other soldier heard suspicious noises outside the truck, and, thinking an enemy soldier was outside, took his carbine, and, contrary to instructions, left the truck unguarded as he went to reconnoiter.

As he was cautiously circling the vehicle, it suddenly was driven off. Consternation! What to do now? General Collins was awakened by his adjutant and informed of the situation -- resulting in a flurry of countermeasures: immediate notification to all Allied forces around the world to change the current setting of the Sigaba rotors, dispatch of search parties, placing all units in the area on alert, and others. Then, next morning, the truck was found on a side road outside town with all the crypto equipment apparently secure and undisturbed within the enclosed vehicle. It could only be presumed that some soldier had decided to take the vehicle for a joyride, not knowing that he had inadvertently chosen one containing Top Secret cryptographic equipment. The two cryptographers who had been on duty in the truck that night evidently were questioned rather extensively and, as I recall, suddenly left our unit for other duty, or perhaps court-martial.

Another unpleasant memory concerns the Red Army commanders we met at Leipzig, after the war had just ended. Collins had arranged a formal meeting with the Russians at the VII Corps headquarters, scheduled for about noon. After waiting on the steps of the large building for several minutes, the general and his staff were astonished to see the Russians roar up at high speed in several open-top long touring cars, with several armed guards standing on the running boards (remember them?) of each vehicle. A disgusting show of arrogance, which certainly dampened the cordiality of the greeting extended to them by the U.S. Army personnel who hosted the meeting.

Our small cryptographic unit normally consisted of about 4 or 5 men, and, naturally, we became a very tightly knit group, each personally as much concerned about the safety of the others as our own, and dedicated to speedy, accurate performance of our cryptographic duties. Unfortunately, that close personal relationship was occasionally severed abruptly by enemy action, with a replacement assigned to our group quickly becoming assimilated. But, to my regret, these relationships eventually and inevitably lapsed after the war, as each of us returned to our homes and again took up our separate civilian lives. I have no information concerning the present whereabouts of any of these men. Perhaps this brief article will be read by at least one of them, leading to a renewal of our friendship. David Waer, George Balog, Dave Berkovich, Stan Kuzminski, Tom Shall — WHERE ARE YOU?

Königswinter - Drachenfels on the Rhine.
Berkovich, Kuzminski, Guelker and Shall.

REAR ADMIRAL JOSEPH N. WENGER USN (RET) AND THE NAVAL CRYPTOLOGIC MUSEUM

ROBERT WELLER

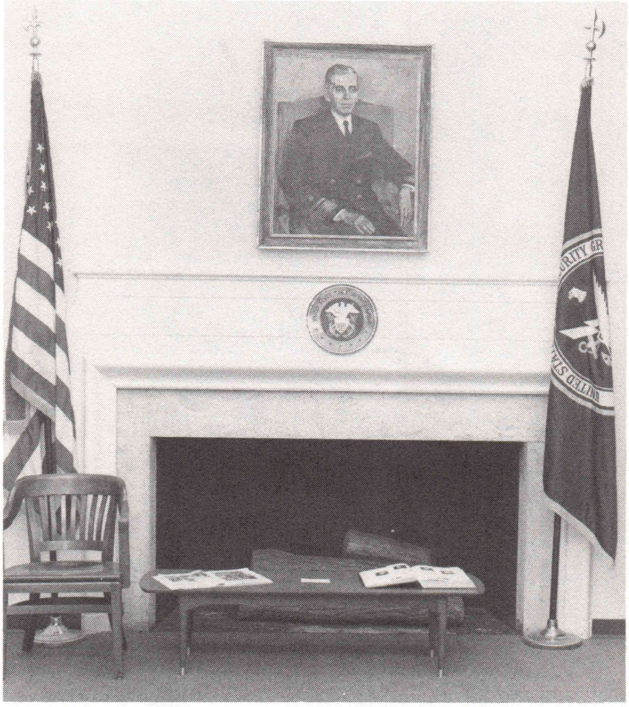
[Editors' Note: When Louis Kruh, one of our editors, learned about the Rear Admiral Joseph N. Wenger Naval Cryptologic Museum, he informed Naval Security Group Command Headquarters that Cryptologia would be interested in featuring an illustrated article on the Museum. As a result, the following article was provided. It gives an abbreviated and fascinating history of the growth and development of some facets of Navy cryptology associated with Admiral Wenger's career.]

Shrouded in security prohibitions, the world of the military cryptologist has for years been one of enforced anonymity. Now operating under fairly recent governmental directives, sincere efforts are being made to raise, where possible, the veil of secrecy which has obscured this vital military function. It is recognized that many significant historical questions, political, military and diplomatic, remain unanswered, and that where the requirements of security are no longer involved, the declassification and release of cryptologic material may help resolve controversies of long standing.

One beneficial effect of this formal declassification program is that it has become possible to offer recognition to certain of the military cryptologists whose contributions have been so vital to the accomplishment of American diplomatic and military objectives.

Thus, in 1976, the Chief of Naval Operations authorized the establishment of the Rear Admiral Joseph N. Wenger Cryptologic Museum, bringing the name and career of the U.S. Navy's first cryptologic Flag Officer to the fore.

Located in the Naval Security Station, 3801 Nebraska Avenue N.W., Washington DC 20309, the Museum was created primarily for the education, inspiration and professional enhancement of Naval Security Group personnel. Although not open to the general public, admission to the Museum by outside groups or individuals may be considered on a case-by-case basis predicated upon sufficient advance application. The Museum provides a suitable setting for the display of materials associated with the history of naval cryptology and electronic warfare. One of its purposes is to foster interest and pride in the many and varied accomplishments which over the years, frequently with little or no positive support or encouragement, made the Naval Security Group an integral part of naval technology and warfare. The Museum also serves to remind one not only of the many technological improvements which have been accomplished within the cryptologic field but also of the men and women who were largely responsible for them.



THE WENGER MEMORIAL CORNER

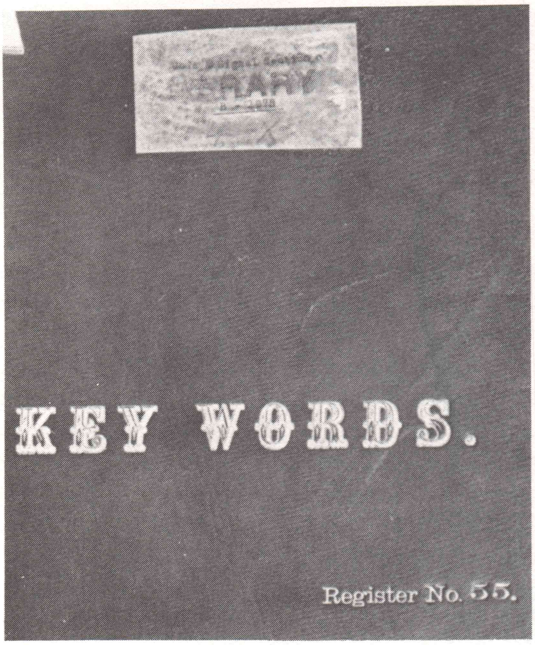
The Wenger Memorial Corner, as its name implies, is devoted entirely to acquainting the visitor with the life of the Admiral. It is one of the most attractive areas of the Museum .

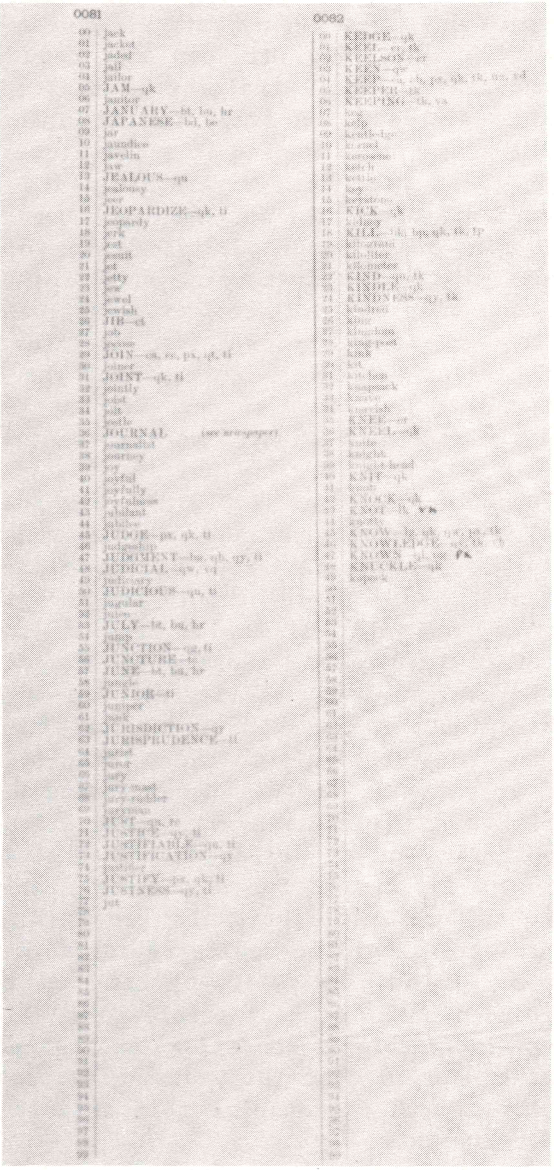
Oil portrait of RADM. Wenger dominates the space. Below is his Academy Yearbook, open to his class picture which provides an interesting contrast to the portrait above.

Momentos from RADM. Wenger's career include photo of his first sea Command (USS TILLMAN--DD 135) (upper right); Decorations and Awards showing (upper right) the Order of the British Empire; also shown are a self-portrait made in 1922 and his sword among other items.

This pioneering group was, on the whole, young, intelligent and dedicated. The officers were mostly Naval Academy graduates who, at best, were seriously jeopardizing their careers by sacrificing professional time at sea for that spent in a new, operationally unproven and, therefore, less than acceptable field. The enlisted personnel were specially selected, first line radio operators of proven worth. Between 1928 and 1941, a total of one hundred fifty Navy Petty Officers and twenty-six Marine Non-Commissioned Officers underwent special training to master the Japanese telegraphic code to permit the intercept and analysis of Japanese radio communications. Because the training was conducted in a restricted classroom on the roof of the Sixth Wing of the former Main Navy Building on Constitution Avenue, Washington DC, the students became known, and are honored in Naval Security Group history, as the "On-The-Roof" Gang. It was this small cadre of less than 200 individuals which laid the foundation for the present Naval Security Group and was the group which contributed so significantly to U.S. successes in the Battle of Midway, the shoot-down of Admiral Yamamoto, the U-Boat defeat in the Battle of the Atlantic and the collapse of the Japanese Navy. Behind these sensational events were hidden the prosaic day-to-day efforts of the many unsung individuals which contributed so importantly to the final victory.

Joseph Numa Wenger (1901-1970) was one of several Radio Intelligence personnel whose contributions and accomplishments were especially influential in structuring a firm foundation for Communications Intelligence and, equally important, in helping to promote its acceptance by skeptical Naval commanders as a valid operational tool. It was men like Rear Admiral Wenger and others equally dedicated, whose perseverance and leadership, despite skepticism on the part of many unbelievers, slowly established a begrudging recognition and acceptance of the operational validity of Communications Intelligence. It was due almost entirely to their tenacity, plus the consistent support provided by a very small handful of far-seeing Senior Officers, that the foundation was laid for the outstanding organization which served the nation to such great advantage during World War II and continues to do so today. As Naval Cryptology's first, and for some years, only Flag Officer, it is fitting that the Museum which reflects the growth in this field from the Civil War to the present, should be dedicated to the memory of Rear Admiral Wenger. By noting some of the high points of his career and the events which preceded or surrounded them, it is possible to develop a greater appreciation of how and why naval cryptologic operations and the processes and equipment employed therein, have changed over the years. The pictorial presentation of some Museum displays which accompanies this article will give additional meaning to these developments.





0081		0082	
00	jack	00	KEDGE—qk
01	jacket	01	KEEL—cr, tk
02	jaded	02	KEELSON—cr
03	jail	03	KEEN—qw
04	jailor	04	KEEP—ca, cb, px, qk, tk, uu, vd
05	JAM—qk	05	KEEPER—tk
06	janitor	06	KEEPING—tk, va
07	JANUARY—bt, bu, hr	07	keg
08	JAPANESE—bd, be	08	kelp
09	jar	09	kentledge
10	jaundice	10	kernel
11	javelin	11	kerosene
12	jaw	12	ketch
13	JEALOUS—qu	13	kettle
14	jealousy	14	key
15	jeer	15	keystone
16	JEOPARDIZE—qk, ti	16	KICK—qk
17	jeopardy	17	kidney
18	jerk	18	KILL—bk, bp, qk, tk, tp
19	jest	19	kilogram
20	jesuit	20	kiloliter
21	jet	21	kilometer
22	jetty	22	KIND—qu, tk
23	jew	23	KINDLE—qk
24	jewel	24	KINDNESS—qy, tk
25	jewish	25	kindred
26	JIB—ct	26	king
27	job	27	kingdom
28	jocose	28	king-post
29	JOIN—ca, ec, px, qt, ti	29	kink
30	joiner	30	kit
31	JOINT—qk, ti	31	kitchen
32	jointly	32	knapsack
33	joist	33	knave
34	jolt	34	knavish
35	jostle	35	KNEE—cr
36	JOURNAL (see newspaper)	36	KNEEL—qk
37	journalist	37	knife
38	journey	38	knight
39	joy	39	knight-head
40	joyful	40	KNIT—qk
41	joyfully	41	knob
42	joyfulness	42	KNOCK—qk
43	jubilant	43	KNOT—tk VA
44	jubilee	44	knotty
45	JUDGE—px, qk, ti	45	KNOW—bg, qk, qw, tq, tk
46	judgeship	46	KNOWLEDGE—qy, tk, vh
47	JUDGMENT—bu, qb, qy, ti	47	KNOWN—ql, vg PA
48	JUDICIAL—qw, vq	48	KNUCKLE—qk
49	judiciary	49	kopeck
50	JUDICIOUS—qu, ti	50	
51	jugular	51	
52	juice	52	
53	JULY—bt, bu, hr	53	
54	jump	54	
55	JUNCTION—qg, ti	55	
56	JUNCTURE—tc	56	
57	JUNE—bt, bu, hr	57	
58	jungle	58	
59	JUNIOR—ti	59	
60	juniper	60	
61	junk	61	
62	JURISDICTION—qy	62	
63	JURISPRUDENCE—ti	63	
64	jurist	64	
65	juror	65	
66	jury	66	
67	jury-mast	67	
68	jury-rudder	68	
69	juryman	69	
70	JUST—qu, tc	70	
71	JUSTICE—qy, ti	71	
72	JUSTIFIABLE—qu, ti	72	
73	JUSTIFICATION—qy	73	
74	justifier	74	
75	JUSTIFY—px, qk, ti	75	
76	JUSTNESS—qy, ti	76	
77	jut	77	
78		78	
79		79	
80		80	
81		81	
82		82	
83		83	
84		84	
85		85	
86		86	
87		87	
88		88	
89		89	
90		90	
91		91	
92		92	
93		93	
94		94	
95		95	
96		96	
97		97	
98		98	
99		99	

TURN OF THE CENTURY COMMUNICATIONS

Cryptographic security of naval messages in the late 1800s and early 1900s depended upon using books correctly. Without both the KEY WORDS BOOK and the U.S. NAVY SECRET CODE BOOK, the cryptographer was unable to complete his task.

The following shows the procedure followed in decrypting a fifteen group message received by the U.S. Naval Attache in Madrid on 12 March 1898. The first four groups of this message were: ABROLHANDO GEOSELENIC ABTRUPPEN DISCONCERT

Step 1: By reference to the KEY WORD BOOK convert each of the above four groups (Keywords) to its numerical equivalent. These are: 00820 00928 28170

Step 2: The five numeral groups are next converted to six numeral groups: 008204 078900 928281 70----

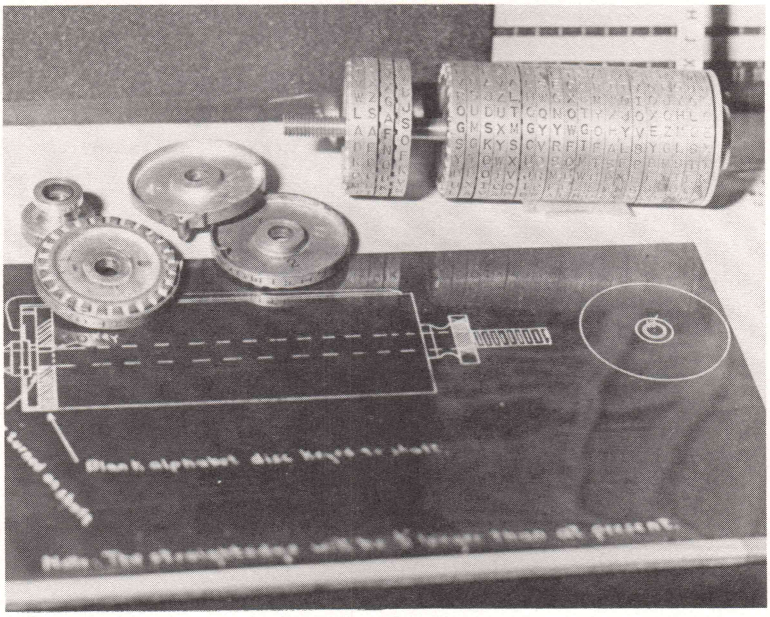
Step 3: English words are next obtained by locating the six digit group in the U.S. NAVY SECRET CODE BOOK (right). The first group, located in the middle column, number "04" translates to "KEEP". The second group, found on another page, translates to "the Department", etc.

The entire message broke out to, "Keep the Department exactly informed when PELAYO and CHARLES V will be ready. Roosevelt."

This system was cumbersome, time consuming and contained numerous opportunities for human error. Nevertheless, the Navy Secret Code was used as a back-up system during World War I.

Most cryptologists, or those interested in the field, are familiar with the beginnings of the modern era of U.S. cryptologic operations under the Army's H. O. Yardley as described in his classic book, "The American Black Chamber." They are equally familiar with his program's progressive demise following World War I, hastened by Secretary of State Stimson's reputed statement that, "Gentlemen do not read each other's mail."

While the United States Navy has been concerned with protecting its signals against unauthorized use since at least the Civil War, modern naval cryptology dates from the period just prior to World War I. Dramatic developments in signals exploitation and security followed the advent of radio communications.


Blank alphabet disc keyed to shaft.
Note: The straightedge will be 3" longer than at present.

CYLINDRICAL CIPHER DEVICE (NAVY CSP 488, ARMY M--94)

This device, used by the U.S. Navy and Army between World Wars I and II, was similar to a "wheel cipher" device invented by Thomas Jefferson in the 1790s but not adopted for encrypting U.S. communications until the early 1920s.

About 700 of the devices were delivered to the Navy in December 1926 for use in the 1927 Fleet Maneuvers. They consisted of a shaft upon which were placed 25 rotatable discs. Each disc had a different alphabet sequence engraved on its periphery and was identified by a number (1-25). Discs were assembled on the shaft according to a Key Word that used these letters and numbers. One Key Word used in 1941 was "THE PAUSE THAT REFRESHES."

The device was designed for use in intercommunications between the Army and Navy, between ships and units of a landing force and between Marine Corps and naval units in the field. Naval Districts also used its as did Fleet Units when prescribed. About 1935 the Coast Guard was added to the list of holders.

Enciphering and deciphering using the device was a time consuming task because only 25 letters could be handled for each setting. Perceptive operators quickly recognized that the device provided little security because the alphabet sequence never changed.

"ON-THE-ROOF" GANG
THE OTRG MEMORIAL
1928
1941
THIS MEMORIAL COMMEMORATES THE 150 US NAVY AND 26 US MARINE CORPS ENLISTED RADIO OPERATORS WHO WERE SPECIALLY TRAINED AT A UNIQUE SCHOOL LOCATED ON THE ROOF OF THE OLD NAVY DEPARTMENT BUILDING DURING 1928-1941 KNOWN AS THE ON-THE-ROOF GANG THEY WERE TRAINED TO INTERCEPT AND ANALYZE FOREIGN RADIO COMMUNICATIONS THIS GROUP OF DEDICATED AND SKILLED OPERATORS FORMED THE VANGUARD OF THE US NAVAL COMMUNICATIONS INTELLIGENCE EFFORTS AND LAID THE CORNERSTONE OF NAVAL CRYPTOLOGY
U S NAVY
U S MARINE CORPS

Adjacent to the Museum, on the Station Quarterdeck, hangs a Memorial commemorating the original 150 U.S. Navy and 26 Marine Corps Enlisted Radio Operators who, from 1928 to 1941, were specially trained to intercept and analyze Japanese radio communications. Known as the "On-The-Roof" Gang due to the location of their classroom on the roof of the Main Navy Building, they were honored on 17 June 1983 by a most impressive ceremony and dedication of a large bronze plaque listing the names of each man who, as the Memorial states, "formed the vanguard of the U.S. Naval Communications Intelligence effort and laid the cornerstone of Naval Cryptology."

Of the ninety living members, thirty-five attended the dedication ceremony.

Almost with the first wireless transmission from a Navy ship in 1899, sailors and Marines assumed duties at sea in newly created radio billets. When USS WYOMING participated in Fleet Exercises in 1913, an energetic and dedicated Fleet Radio Officer, Lieutenant S. C. Hooper, was serving in the Atlantic Fleet Flagship. His constant urging that the Navy adopt the new method of "wireless" communication resulted in his assignment to WYOMING where he quickly demonstrated the two-edged potential of the new process. By comparing signal strengths, tones and operator characteristics, he successfully predicted the time of attack four hours before it began. Hooper later became Director of Naval Communications and a staunch advocate of Naval cryptology.

RIP-5 (UNDERWOOD CIPHER MACHINE)

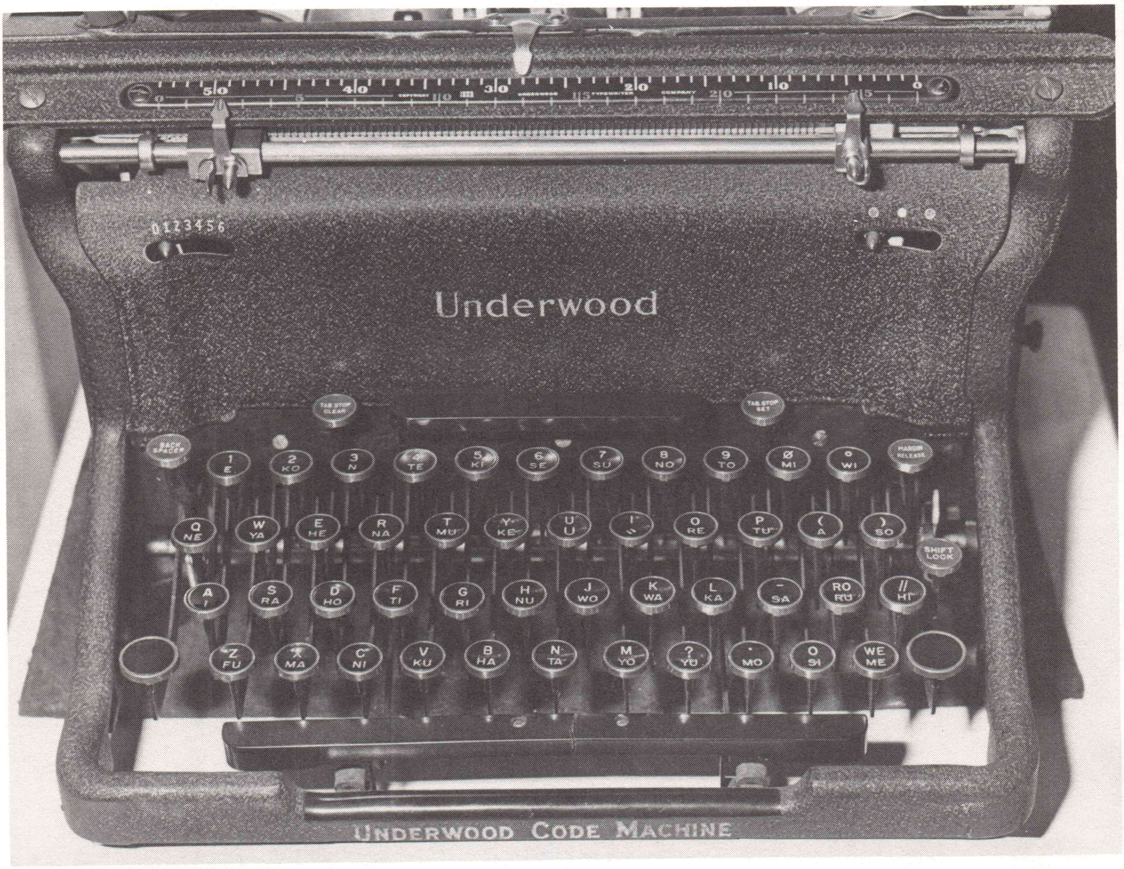
(opposite)

Prior to 1925 Navy Intercept Operators copied Japanese radio messages by hand. In the early 1920s only one Radioman could reproduce the Kana characters manually and only one other could read them. An important step in establishing an Intercept Service was taken in 1924 when Lieutenant Laurance F. Safford, the first naval officer to fill a Cryptologic billet, in consultation with the Underwood Typewriter Company, drew up design specifications for a "special code machine." These were furnished to Underwood and, on 10 December 1924, four machines were ordered at cost of $161.25 each.

Known in its early life as the Underwood Code Machine, the RIP-5 was the regular typewriter normally furnished for radio circuit operators but with type faces which printed "Kana" characters (in Japanese brush-stroke form) instead of Roman letters. The Lower Case typed the Kana ideograph character while the Upper Case typed two additional characters, Japanese Accent marks, English capital letters, arabic numerals and English punctuation marks. The 1924 model carried 46 Japanese-English keys with characters similar to those shown in the photograph. The Roman character equated to the Kana digraph seen on the key with it. Together with the Electric Coding Machine (ECM) and the IBM Sorting equipment, the RIP-5 was one of the three most important ancillary equipments in the field of Cryptologic Operations.

One of the first four RIP-5s was sent to the USS HURON, Flagship of the Chief, Asiatic Fleet; numbers two and three were sent to the only Navy Shore Intercept Station existing in 1924 -- Shanghai, China. The fourth was held by the Code and Signal Section in Washington for training.

Prior to 1917, the Navy undertook sporadic efforts to develop or apply the new technology to fleet operations. For all practical purposes, the history of naval cryptology begins with our entry into World War I. Navy codes and ciphers of that time were clumsy and time-consuming to operate; some of them dated back to the days of sail simply because no trained Navy personnel were available to improve them. During the War, the Code and Signal Section of Navy Communications compiled, produced, distributed and accounted for all codes and ciphers in the Navy. The Section relied heavily on the British Admiralty for advice concerning the construction of more secure cryptographic systems. Little is recorded of U.S. signals intelligence activity, but it has been learned that shipboard intercept was attempted and may have been successful. Although the Navy Department did not process or report on intercepted messages, it did establish a system of medium frequency Direction Finding stations along the Atlantic Coast to track German U-Boats. These stations were later diverted for use as aids to navigation and subsequently turned over to the Coast Guard.



Following World War I, the Navy realized that naval warfare had been vastly affected by communications-electronics. In July 1922, the Navy cryptologic element in OPNAV was designated OP-20G, a title retained until after World War II. To this day the Commander, Naval Security Group Command is designated by the letter "G," a direct relationship to OP-20G. During the next ten years, OP-20G served as a bridge between Naval Communications and Naval Intelligence marking a period of teamwork and enormous technological growth. In Communications Security the Navy recognized the future lay in machine cipher systems and sponsored the development of electrically powered equipment to replace the hand-operated Strip Ciphers devised in 1917 and 1918.

In the early 1920s, an important step was taken in the process of setting up an Intercept Service when a Cryptologic Research Desk was established in the Office of Naval Communications. Conflict exists as to the date of establishment, but Lieutenant Laurence F. Safford, USN, who reported on 5 January 1924, is generally regarded as the first incumbent. With the exception of time spent at sea to maintain his qualifications for promotion, almost his entire career from the mid-20s until retirement in 1952 was spent with the Communications Intelligence organization. He taught himself the principles of the new science, established a system for selecting and training personnel for the highly classified duties, contributed significantly to the development of new time-saving equipments and organized a number of stations to provide Direction Finding and intercept capabilities while coordinating the operation and administration of the entire organization from his post in Washington.

THE HEBERN CIPHER MACHINE

(opposite)

An early electric coding machine was developed and patented by its inventor, Edward S. Hebern, in 1921. He offered to sell it to the Navy and submitted it for test. Miss Agnes Mae Meyer (later Mrs. Agnes M. Driscoll) referred to as "the Navy civilian who instructed Lieutenant Laurance F. Safford in the cryptanalytic art," succeeded in recovering the cipher sequence and method, much to Hebern's chagrin.

According to RADM. Wenger, he understood that Mrs. Driscoll had been lured away from the Navy for some period between 1920 and 1925 to work for Hebern and improve his machine which she apparently did. Where she worked and for how long is unknown.

Although other machines were developed in the 1930s by naval personnel and using wired rotors were used in the Fleet, the Navy issued a number of Hebern machines (32) and used them as its primary machine until supplanted by the ECM in the mid-30s. An undated, anonymous note in the files states, "The machine submitted by him (Hebern) went through a long process of change in design and construction so the final model as issued contained very little of the ideas of the basic device -- however, the name was still used." The machine as finally issued to the Navy was known as the HCM MK II and carried the Short Title CSP 903.

An important step in establishing an Intercept Service and one of Safford's major contributions occurred in 1924. At that time, in consultation with the Underwood Typewriter Company, he drew up the design specifications for a special "Underwood Code Machine," later known more familiarly as the RIP-5

(Radio Intelligence Publication - 5). Prior to 1925, Navy Intercept Operators copied Japanese messages by hand. The new machine now made available to them was the regular typewriter normally furnished to operators but with a vast improvement -- type faces on the type bars which printed the "Kana" characters used in Japanese radio communications. The new procedure was quite simple. An operator hearing the Morse combination -... (B) would strike the key which normally printed the English "B." on The RIP-5, instead of "B," printed the appropriate "Kana" character. The new machine, which was to become standard throughout the Navy Radio Intelligence organization, significantly reduced the training time for Intercept Operators, greatly improved the legibility of copy and served to increase the volume of traffic which could be transcribed. The original machines cost $161.25 each and one of the first four remained in service until, at least, World War II. As of 7 December 1941, OP-20G had purchased 127 RIP-5s, and by war's end there were more than 1600.

It was during this formative and historic period that Ensign Wenger first became associated with Naval Communications Intelligence. In 1969, he wrote the following account of how this came about:

"On November 1924, I was ordered to 'temporary duty under instruction' in the Office of Naval Communications. Curiously enough, the reason for my selection for this assignment was that the Captain of my ship, who had been directed to send one Ensign there, had learned that my family resided in Washington, and he felt that I was the only one among those eligible who could live there on an Ensign's pay. In retrospect, it seems incredible that my entire career was decided by that simple and essentially irrelevant circumstance."

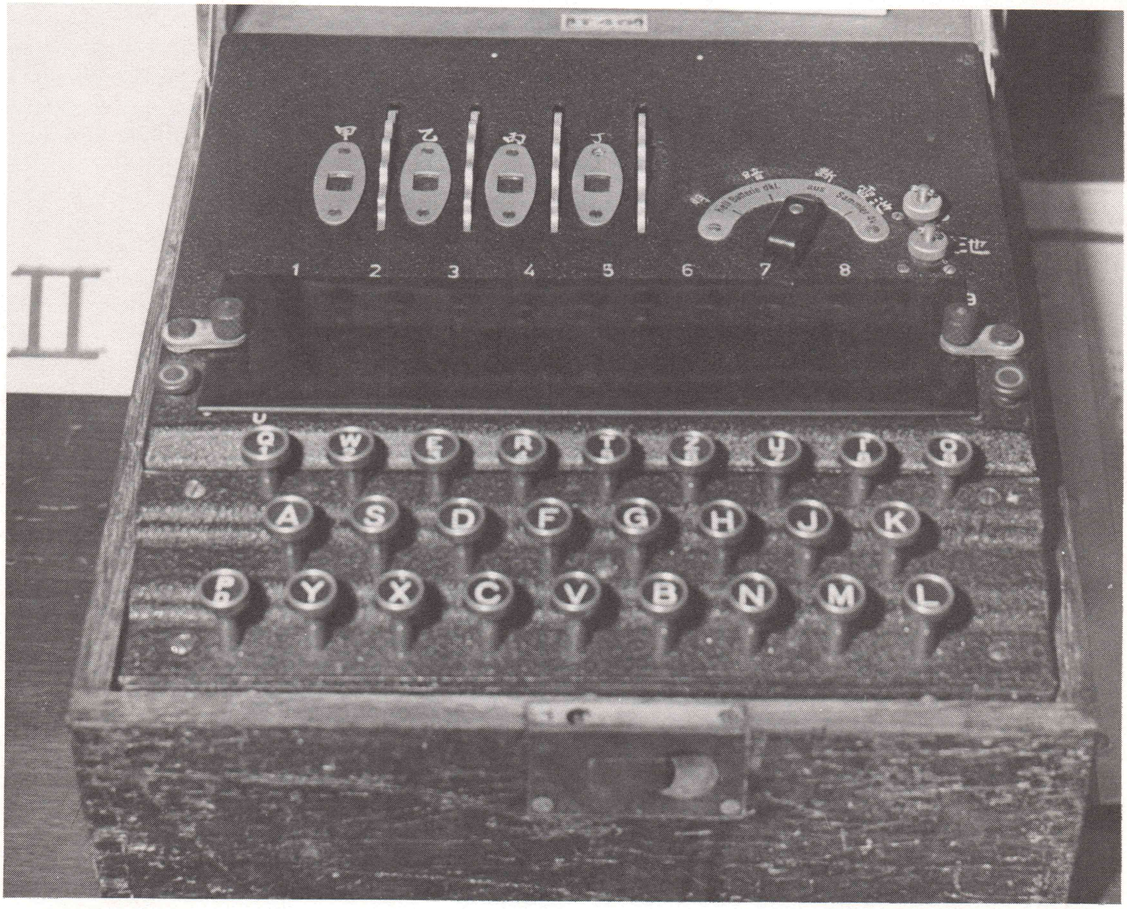
ENIGMA MACHINE

(opposite)

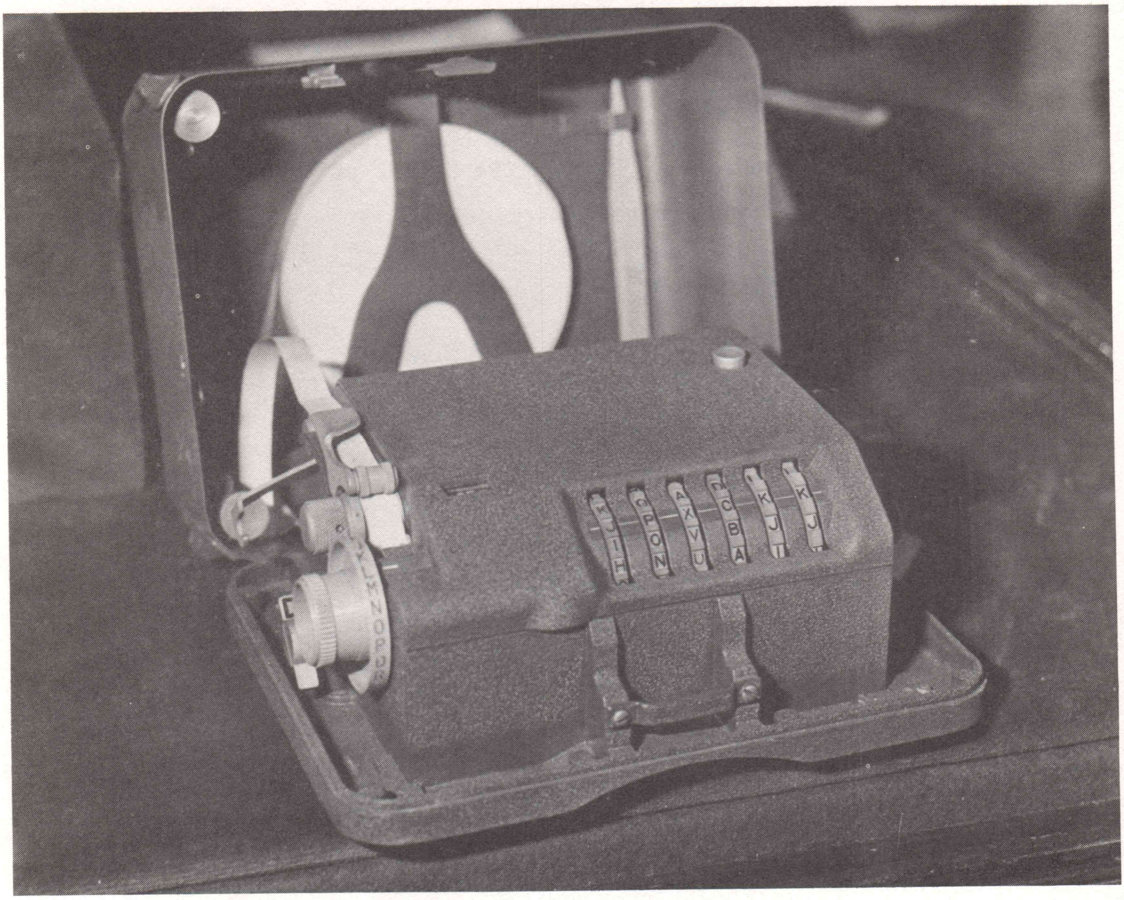
This device, originally conceived by a Dutchman, was perfected by a German, its system initially broke by the Poles and its more complex World War II systems read consistently by the British. The Germans' unshakable faith in the security of Enigma led to its continued use throughout the war during which time approximately 100,000 machines were constructed by the Third Reich.

After a brief tour in the Navy Department Code Room, Ensign Wenger was sent to the Research Desk where he was given some material on cryptanalysis to study, none of which aroused much of his interest since his training thus far in the

Navy had pointed him towards a career in gunnery. While studying this material, he was pressed into service, "being the nearest spare pump handle," as he put it, to help straighten out the badly confused accounting records in the Registered Publications Section and later to fill an unexpected vacancy among the Departmental Communications Watch Officers. After ten months in Washington, he returned to sea as a Communication Watch Officer on the staff of Commander Battleship Divisions. He felt that this brief Washington experience was what led to his return there in 1930 to take the expanded 12 month course in Cryptanalytic Training and his later specialization in Communications Intelligence. His tour also possibly formed the basis for the curriculum drawn up by Safford for the first course in 1925, as later students followed the same general pattern of assignment in the Office of Naval Communications.



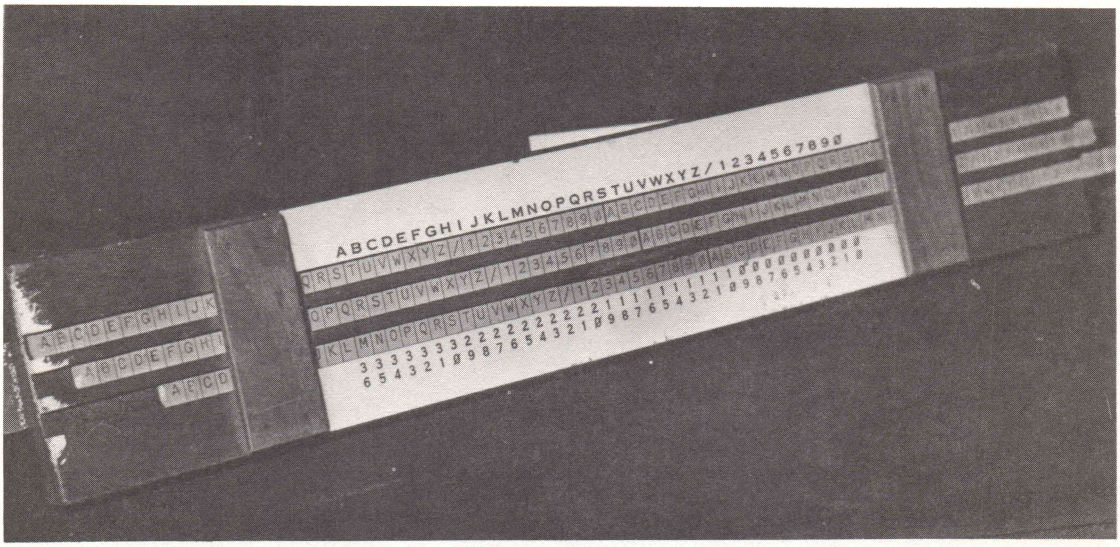
In June 1931, the Bureau of Engineering, which had been given responsibility for the development of mechanical devices for Ciphering and Recognition Systems, stated it needs for an officer to head the cognizant section. This individual was required to have expert knowledge regarding the subject of cryptology. Now a Lieutenant, Wenger was identified as "the only officer with the requisite qualifications who is available for this assignment at this time." He was detached from the Office of Naval Communications at the end of June, and while on leave during July, inspected such activities as RCA Communications, Bell Laboratories, General Electric and Sperry Gyroscope.



HAGELIN CIPHER MACHINE

Invented by Boris Caesar Wilhelm Hagelin in the 1930s, this machine is still manufactured and sold commercially. The Swedish inventor relocated his plant to Switzerland after World War II.

This machine was acquired by the U.S. Army and Navy for use during World War II. The two versions were virtually identical, compact, rugged and provided a reasonable secure but slow manual means of encryption.

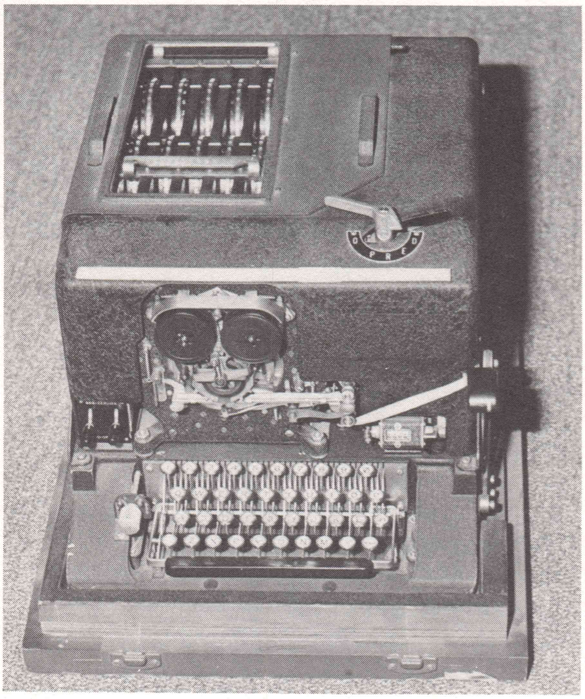


CALL SIGN ENCRYPTION

The CSP 1756 Call Sign Encryption Device was used extensively in World War II. This Strip Cipher System was one of several methods used for the encryption of Call Signs. It was retired from active service in 1961 after nearly 20 years of use.

At the end of his year with the Bureau of Engineering, Lieutenant Wenger was sent to Europe where he investigated and reported on several cipher machines including the O'Brien Cipher Machine (England), the Belin Cryptographic Machine (France), the Aberly Cipher and Method of Cipher Solution (Switzerland), and Enigma (Germany). In 1970 Rear Admiral Wenger summarized these investigations as follows:

"The O'Brien Machine was a cleverly designed mechanical device consisting of a series of interchangeable, geared cipher wheels and a stepping mechanism. The cipher was changed by rearranging the order of the wheels and resetting them according to a key. The Belin machine was of special interest as it was the first device for encryptive facsimile of which we had any knowledge. While I was in Paris, test transmissions were being sent from the Eiffel Tower. As for the Enigma, little did I then dream of the trouble it would later cause us in World War II. Upon my arrival in Berlin, the Naval Attache, Captain Castlemen, insisted on notifying the Ministry of Marine of my interest in the Enigma, although the machine was being produced and openly advertised by a commercial company. Upon visiting the factory the following day, I was told that the German government had just put restrictions on the device so that it could not be shown to me. However, the Company representative interpreted these instructions liberally and showed me slides of the mechanism which clearly revealed its nature. What I really wanted was a long sequence of copied text produced from a single letter input. This, unfortunately, I was unable to obtain without access to the machine. The ABEL (sic) cipher turned out to be simply a random additive key of infinite length which the inventor claimed could be produced from a logarithmic table."



ECM (ELECTRIC CIPHER MACHINE)

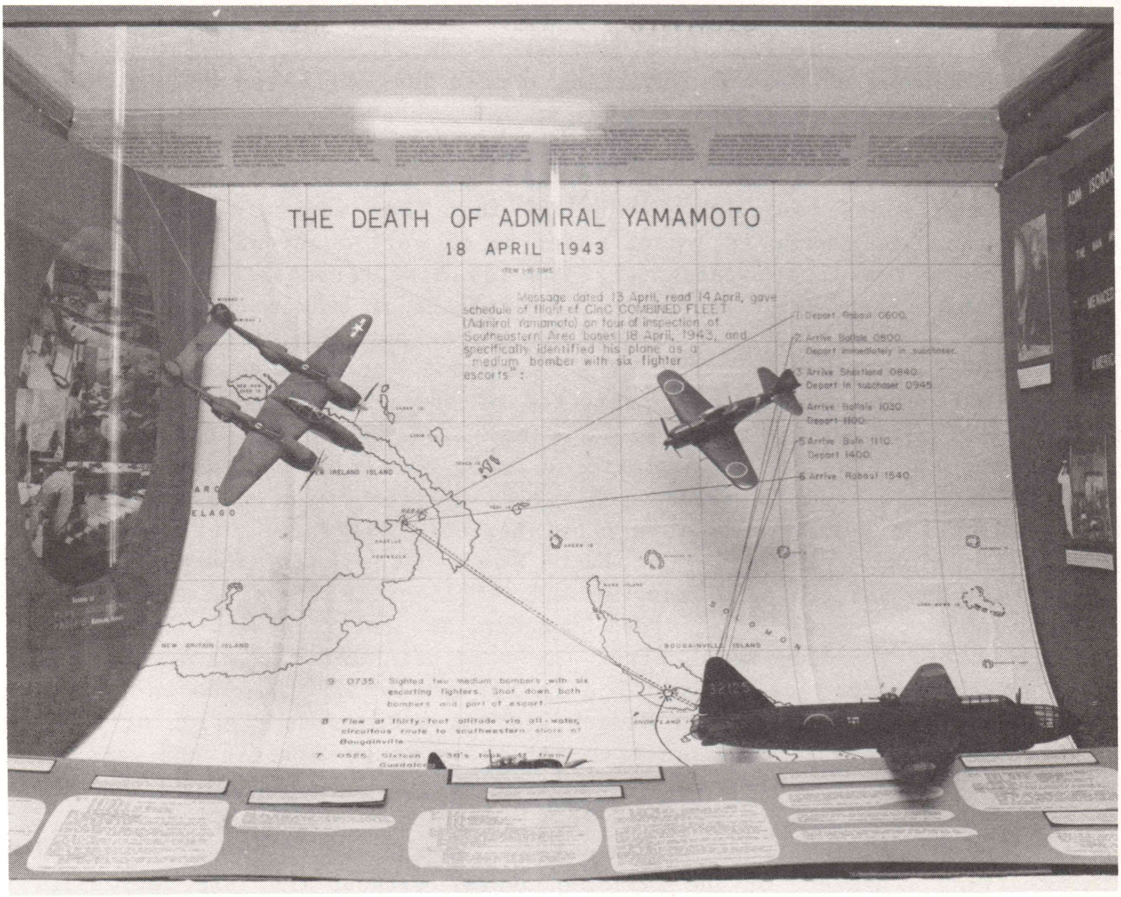
Developed during the 1930s, the ECM had been distributed to the U.S. Fleet by the outbreak of World War II. It served throughout this conflict as the primary U.S. machine system. It was used as well during the Korean affair. Known by its short title as the CSP 889/2900 this model had the capability to accommodate Combined communications involving our Allied holders. It was partially due to the perfection and improvement of the rotor machine that Friedman, Safford and Rowlett each won $100,000 grants from the Government of the United States.

From his European trip Lieutenant Wenger proceeded to the Asiatic Station where, on 25 June 1932, he took over the assignment of Asiatic Fleet Radio Intelligence Officer. As a follow-up to the limited coverage which had been made of the 1930 Japanese Naval Maneuvers, Lieutenant Wenger made plans for an even more complete coverage of the Grand Maneuvers of 1933. Captain Safford's 1943 history gives the following account of this important event which led Lieutenant Wenger to some far-reaching conclusions with respect to our own Navy's vulnerability to Traffic Analysis:

"The 1933 Maneuvers followed the magnitude and general pattern of the 1930 Grand Maneuvers and confirmed our belief that they were a rehearsal of war plans. We had much more intercept material to work on because our operators were more numerous and experienced, and the maneuvers lasted longer so the information was considerably greater. The lessons of 1930 were not wasted and plans were made well in advance for the secret participation of the Asiatic Radio Intelligence Units in the 1933 Maneuvers. At that time, the Asiatic Radio Intelligence Organization consisted of one officer and 30 men, all of whom participated in the maneuvers, as compared with nine men who covered those in 1930. Personnel were scattered among four widely separated stations which permitted a greater variety and amount of intercepted messages but made the coordination difficult and entailed serious delays in getting intercept logs to the points where they could be used. Lieutenant Wenger remained aboard the Fleet Flagship in Tsingtao and, while estimates from the intercept stations were occasionally forwarded by radio, the intercept logs for the most part did not reach him until after the conclusion of the maneuvers. This delay was 'constructively' canceled in his analysis. Due to the lack of clerical assistance, Lieutenant Wenger did not attempt decryption of problem traffic but gave a full-scale test to our theories of 'traffic analysis.'"

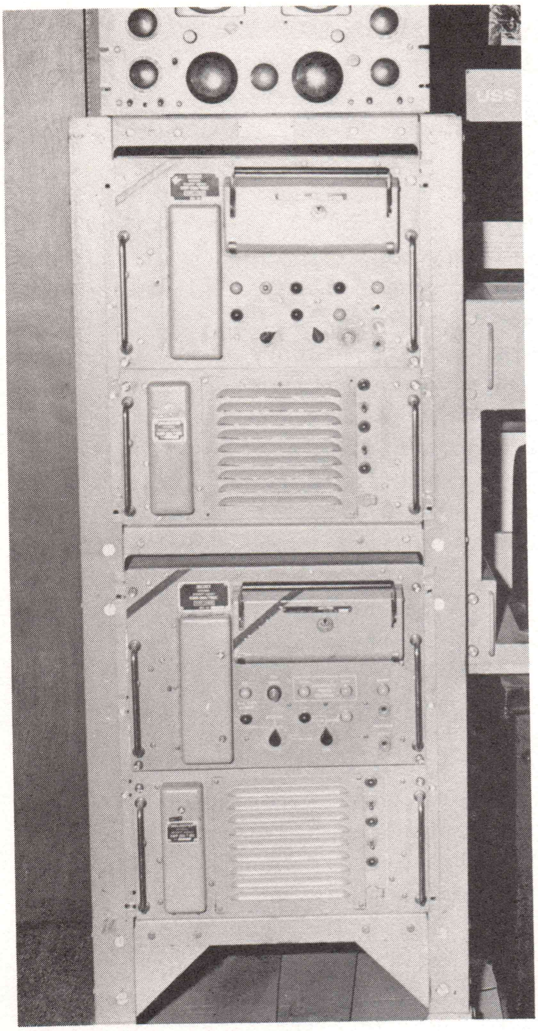
Commander-in-Chief Asiatic Fleet's final report was not completed until the spring of 1934 and consisted of 115 pages. The success of the Traffic Analysis in giving a picture of the 1933 Maneuvers, without the information later obtained from decryption, completely sold the idea of Radio Intelligence to Admiral Upham, Asiatic Fleet Commander. In 1970 Rear Admiral Wenger wrote, "In my view the 1933 Maneuvers proved to be as important a turning point in the affairs of OP-20G as had been the 1930 maneuvers. The results achieved in the latter had made a great impression on, and garnered important support from, Senior Officers in the Navy. The question inevitably arose after the 1930 maneuver as to how much reliance could be placed upon COMINT since cryptographic systems could certainly be changed by the enemy and considerable time would be required to make them readable again. How could loss of source and time be overcome? Results of the 1933 Maneuvers lessened, if not largely dispelled, these misgivings. By demonstrating through Traffic Analysis that valuable information could be obtained from communications by methods short of

cryptanalysis, and especially by exploiting aspects of communications that are not readily changeable, a new dimension was added to COMINT. Furthermore, a new hazard to our own communications security was revealed."


THE DEATH OF ADMIRAL YAMAMOTO
18 APRIL 1943
Message dated 13 April, read 14 April, gave schedule of flight of CinC COMBINED FLEET (Admiral Yamamoto) on tour of inspection of Southeastern Area bases 18 April, 1943, and specifically identified his plane as a "medium bomber with six fighter escorts":
1 Depart Rabaul 0600
2 Arrive Ballale 0800 Depart immediately in subchaser
3 Arrive Shortland 0840 Depart in subchaser 0945
4 Arrive Ballale 1030 Depart 1100
5 Arrive Buin 1110 Depart 1400
6 Arrive Rabaul 1540
9 0735 Sighted two medium bombers with six escorting fighters. Shot down both bombers and part of escort
8 Flew at thirty-foot altitude via all-water, circuitous route to southwestern shore of Bougainville
7 0525 Sixteen P-38's took off from Guadalcanal
NEW IRELAND ISLAND
NEW BRITAIN ISLAND
BOUGAINVILLE ISLAND
32125

THE DEATH OF ADMIRAL YAMAMOTO

In April 1943, based on information provided by Navy Communications Intelligence, the Commander-in-Chief, Japanese Combined Fleet, Admiral Yamamoto, was shot down and killed en route to an Inspection in the Bougainville area. After the Battle of Midway, this event was, up to that time, the most sensational accomplishment based on information originating from Communications Intelligence sources. The message from Hawaii which provided the tip-off ended on a highly suggestive note, "Tallyho. Let's get the Bastard!" This display in the RADM. Wenger Museum describes the affair in detail.



KW-26

Successor to the ECM (Electric Cipher Machine) and one of the first in a new family of non-rotor crypto devices on which the security of U.S. encrypted communications depended while even more unique and secure systems were being perfected.

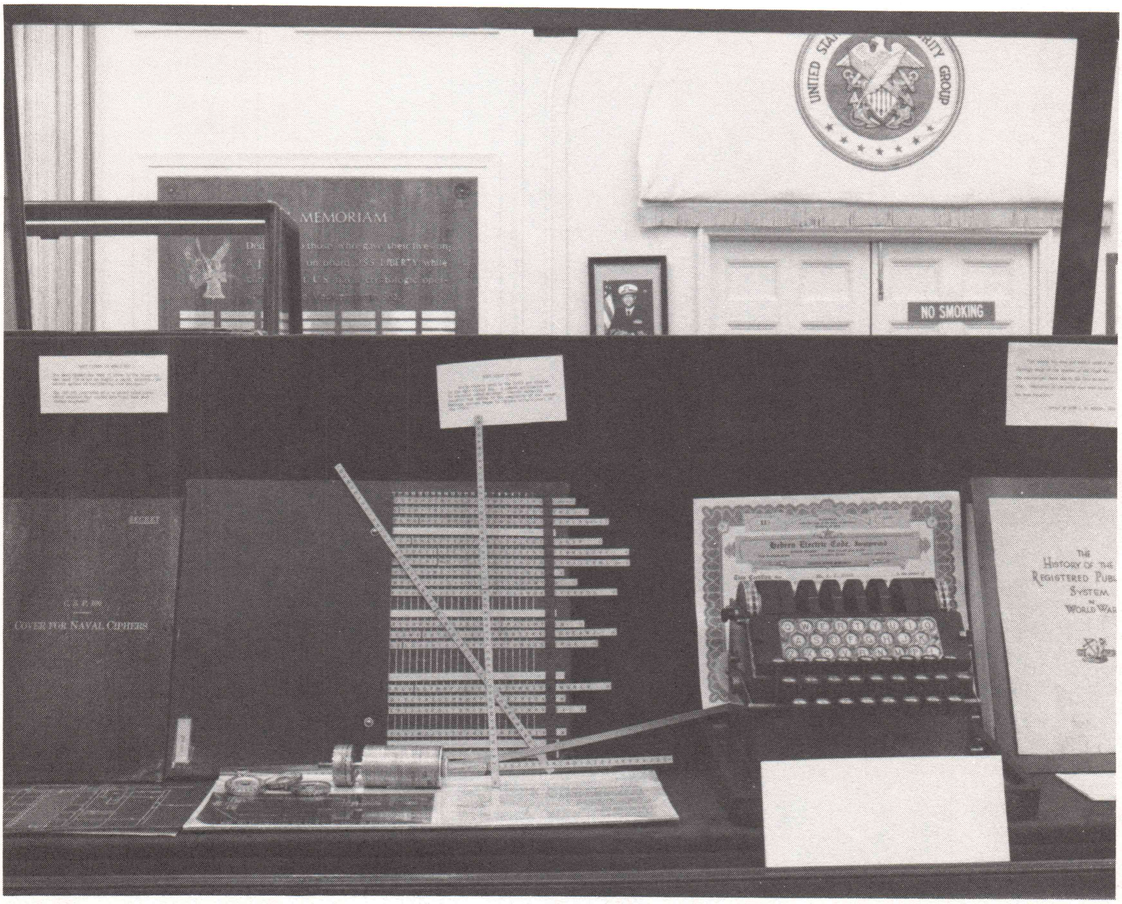
Wenger was only one of many experts who became convinced that the sole answer to time-consuming codes and their encryption was a new philosophy founded upon the discarding of coding in favor of ciphering. In 1935, he proposed investigating the feasibility of developing special cryptanalytic machinery and suggested that some fresh method of attack might be identified from scientists who were working on certain problems analogous to OP-20G's.

Some few months after Lieutenant Wenger had reported to OP-20G in 1935, Lieutenant Commander Safford returned from sea to once again take over the organization, a position he was to hold during the next six years. Both men were intellectually curious, scientifically and technically inclined and adept at recording their thoughts on paper. Consequently during 1937 and 1938, Lieutenant Wenger and Commander Safford (he had been promoted in August 1937) addressed themselves to numerous aspects of the Communications Intelligence scene and to its obverse, Communications Security.

A 30 June 1937 "Military Study of Communication Intelligence Research Activities," authored by Wenger, was a comprehensive study of all elements of law, regulation and policy which bore on the Communication Intelligence mission and an analysis of the problems which this mission presented. His "Military Study of Secret Radio Calls" discussed the value of such calls and drew upon the experience of the Radio Intelligence organization in reconstructing the Japanese Maneuvers of 1930, 1933 and thereafter, especially the work done in Traffic Analysis, to extract information without access to the test of encrypted messages. It pointed out the type of information available from the headings of messages alone if the call sign system could be solved and from the routing and relay of messages within the communications net involved. This study was the base upon which several experiments with secret calls in the U.S. Fleet were carried out in the nearly four years before Pearl Harbor, and furnished many of the criteria for establishing the form of the call sign ciphers which was developed and for evaluating their usefulness after trial. It also inspired (or challenged) Wenger to develop a mechanical Call Sign Cipher device which was adopted by the Navy to replace some of the more time-consuming and cumbersome Strip Ciphers.

At Safford's recommendation, studies were made of several communication systems being used commercially -- High Speed Morse, Radio Teletype, and Facsimile -- in the belief that their use would mean a great increase in circuit capacity and, at the same time, reduction in the manpower required to operate them. Lieutenant Wenger's "Military Study of Facsimile" concluded it was unlikely Facsimile would supplant Morse or its equivalent for reasons including dependability, bandwidth, security, the need for synchronization and the additional equipment required. He recommended, however, that developments be studied so we would be prepared against its use by a future enemy.

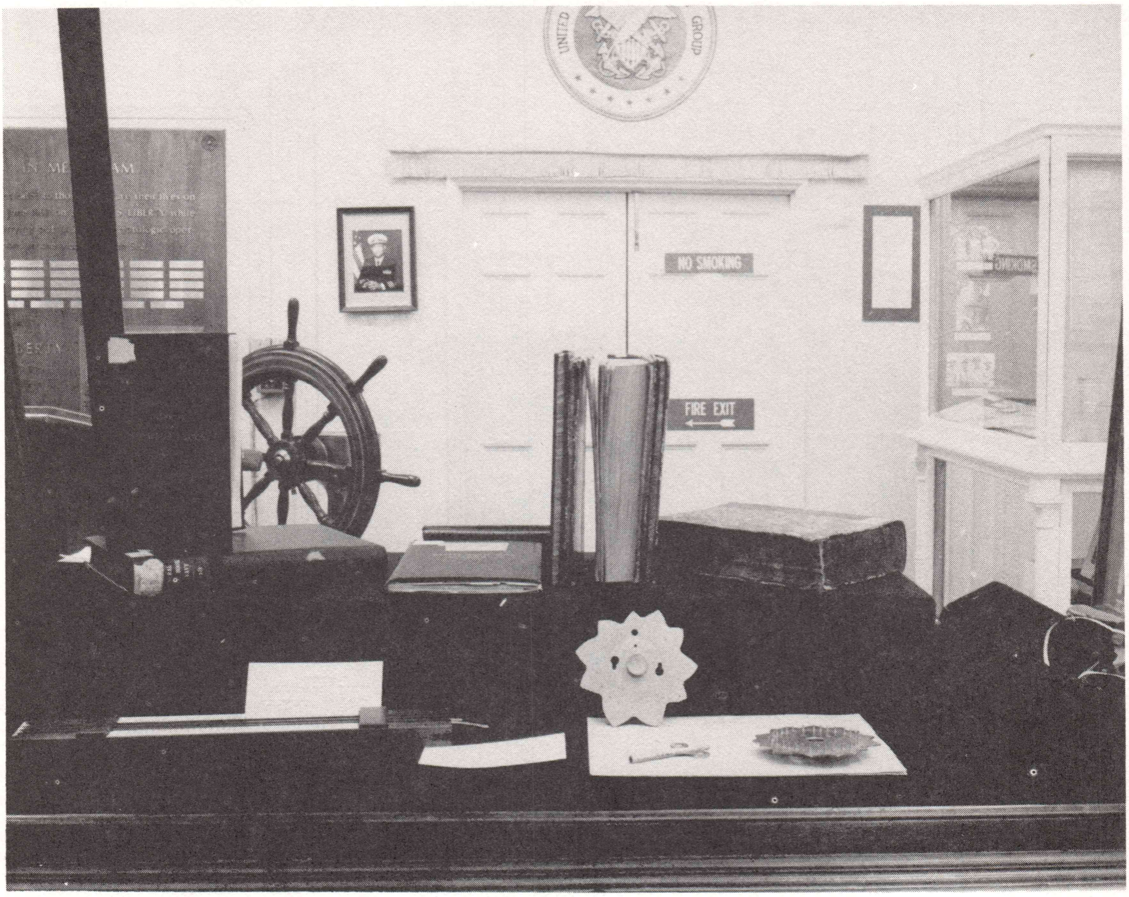
Meanwhile, methods were being developed for using IBM equipment for speeding up many of the critically slow processes involved in decrypting the huge volume of Japanese Naval messages being intercepted. A 1 April 1938 paper by Wenger proposed a mass method of decoding messages which was later adopted and used extensively during World War II in Washington, Pearl Harbor, Melbourne and, to some extent, at collaborating British stations in the Pacific. In 1970, Rear Admiral Wenger noted that, "this was the first generally applicable method of automatic mechanical decryption known to be used in cryptanalysis. It proved of immense value in the rapid scanning of bulk traffic to determine priorities for further processing and in code recovery to assist in hole filling." With this final contribution, the now Lieutenant Commander departed, on 30 June 1938, for a tour of duty at sea. He was not to return to Communication Intelligence duties until 1942.


UNITED STATES NAVAL SECURITY GROUP
MEMORIAM
NO SMOKING
SECRET
C.S.P. 1100
COVER FOR NAVAL CIPHERS
Hebern Electric Code, Incorporated
THE HISTORY OF THE REGISTERED PUBLICATION SYSTEM IN WORLD WAR

MUSEUM DISPLAYS

Two display cases give a broader view of the Museum and a different view of some items shown in individual pictures. In one case (left) may be seen the Cylindrical Cipher Device, a Strip Cipher and Hebern Cipher Machine. In the other (right), the CAMS Zig-Zag Device which enables a Helmsman to steer a sinuous course and the Call Sign Cipher (Strip) Board are below several early Code Books and Communications Regulations going back to the Civil War Period.

The OP-20G to which Commander Wenger then returned was an entirely different organization from that he had left four years earlier. The tremendous wartime increases in personnel, field stations, message volume, demands for COMINT product (not to mention the increased reliance placed on it) required a much more complex and less personal management than had previously been the case.



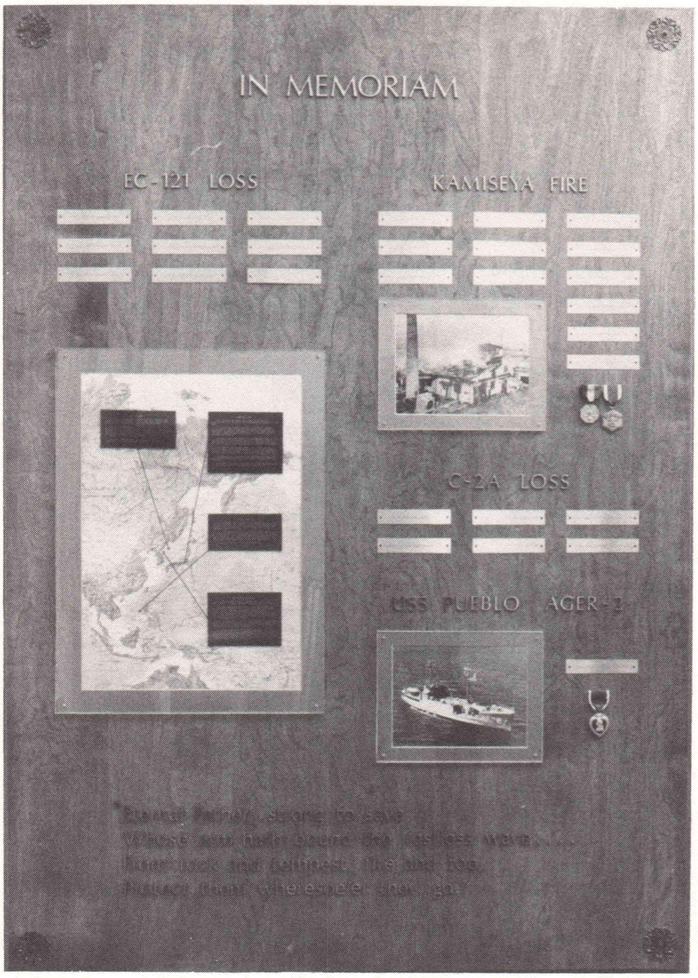
The photo in the background is that of Captain Wm. L. McGonagle, USN, Commanding Officer of LIBERTY, the Research Ship attacked by the Israelis during the Seven Day War. For his bravery under fire and his handling of his ship, the captain received the Congressional Medal of Honor. The Ship's Wheel and the LIBERTY Memorial are adjacent to the Captain's photo.

Gone forever were the days when the group was small and one could know, or have a nodding acquaintance with, its several hundred members. New conditions required more centralized and coordinated methods of operation. Faced with the pressure of wartime operations and a fast-growing, willing but largely inexperienced team of "civilian" sailors, the situation left no time for technical thesis or theoretical expositions. Less than two months after Pearl Harbor, the first breakup of the Code and Signal Section, OP-20G, since its inception in World War I was directed. For the first time in U.S. Naval History, Communications Security was divorced from Communications Intelligence, and they remained separated until after the war.

Wenger remained in the Washington Headquarters throughout the war and was responsible for directing the technical and planning aspects of an organization which, in addition to that Headquarters, encompassed two major field collection units in Hawaii and Australia and, at times, almost forty smaller Direction Finding and Intercept stations located throughout the United States, in Alaska, Greenland, the Caribbean and the South Pacific. Promoted to Captain in 1943, Wenger was designated Deputy Director of Naval Communications and Head of OP-20G in November 1944, a position he was to hold until 1949.

After the Allied victories in Europe and the Pacific, the Navy was reduced in size and consolidation of functions became necessary, even for Naval Cryptology. Increasingly complex technology and more sophisticated equipment added new responsibilities and accelerated the movement toward career specialization. In 1948, Officer designators and enlisted ratings were established for Naval cryptologic personnel. Closer alliance with Army and Air Force Cryptologists was formalized in 1949 with the establishment of the Armed Forces Security Agency to which Captain Wenger reported as Deputy Director in July of that year. In 1951, he was nominated and confirmed as Rear Admiral, the first Navy Cryptologic Flag Officer. Shortly thereafter, he was named Vice Director of the National Security Agency which replaced Armed Forces Security Agency as the nation's guiding cryptologic organization. For his services in this position Admiral Wenger, upon transfer, was awarded the National Security Medal by the President of the United States for outstanding performance of duty and exceptional contributions to the national cryptologic program.

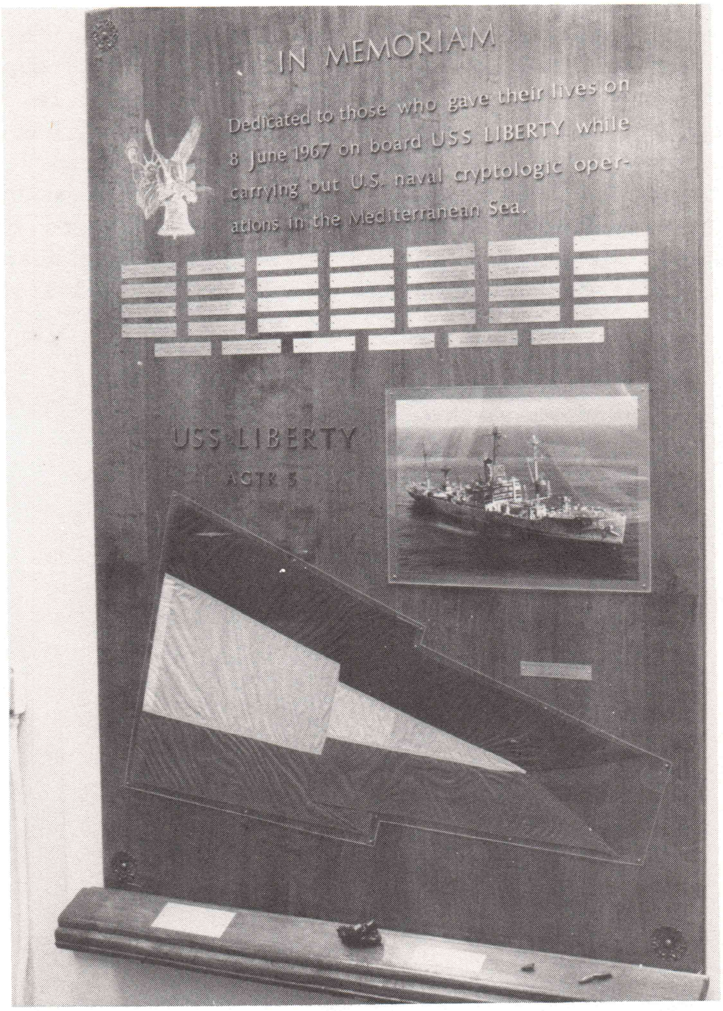
On 1 February 1958, after thirty-five years of active Naval duty, Rear Admiral Wenger was transferred to the Retired List of the U.S. Navy. In addition to the National Security Medal, the Admiral, during these years was awarded, amongst others, the Distinguished Service Medal; Navy Unit Commendation Ribbon; Yangtse Service Medal; the European-African-Middle Eastern Service, Asiatic-Pacific Service and American Campaign Medals. He was also awarded the Order of the British Empire (Honorary Commander) by the Government of Great Britain. These and the remainder of his awards are on display in the Museum.


IN MEMORIAM
EC-121 LOSS
KAMISEYA FIRE
C-2A LOSS
USS PUEBLO AGER-2
"Eternal Father, strong to save
Whose arm hath bound the restless wave, ...
From rock and tempest, fire and foe,
Protect them wheresoe'er they go."

IN MEMORIAM

That cryptologic assignments in the military are not without their dangers is poignantly reflected in the several Memorials displayed in the Museum.

A fire in the Operational Area of the Naval Security Group Activity Kamiseya, Japan, in September 1965, resulted in the deaths of twelve men. Bombed and strafed by Israeli planes during the Seven Day War in June 1967, the USS LIBERTY, a Naval Security Group Research Ship, in a case of "mistaken identity," suffered the death of 33 naval and one civilian personnel.


IN MEMORIAM
Dedicated to those who gave their lives on
8 June 1967 on board USS LIBERTY while
carrying out U.S. naval cryptologic oper-
ations in the Mediterranean Sea.
USS LIBERTY
AGTR 5

Well known is the story of USS PUEBLO, another Research Ship, captured by the North Koreans in international waters, in May 1967, with the loss of one life and the incarceration of seventy-two crew members. In April 1969, an unarmed EC-121 Aircraft was shot down over the Sea of Japan, in international waters, by North Korean fighter aircraft, with the loss of nine Communication Technician (CT) lives. Another six CTs, en route to duty in Viet Nam from the Philippines, and four crew members died when their plane disappeared, presumably at sea. Then, in December 1979, a busload of sailors was attacked in Puerto Rico, resulting in the deaths of two men, and the wounding of ten others. The Museum honors the memory of these brave and dedicated officers and men whose lives were sacrificed in the service of their country.

Rear Admiral Wenger's "Military Studies" provided a basis, within the Cryptologic community, for specific action, experimentation or philosophical contemplation. His periodic duties afloat kept him aware of the role COMINT should play in assisting at-sea Commanders to make valid operational decisions. As a working cryptanalyst and traffic analyst, Staff Assistant and Head of several operational sections, he gained during peacetime the professional knowledge which helped Naval cryptology so successfully accomplish its mission during wartime. It is most fitting that the U.S. Naval Cryptologic Museum, the first of its kind, should be dedicated to the memory of Rear Admiral Joseph Numa Wenger, USN.

A VIEW OF RENAISSANCE CRYPTOGRAPHY - A BOOK REVIEW

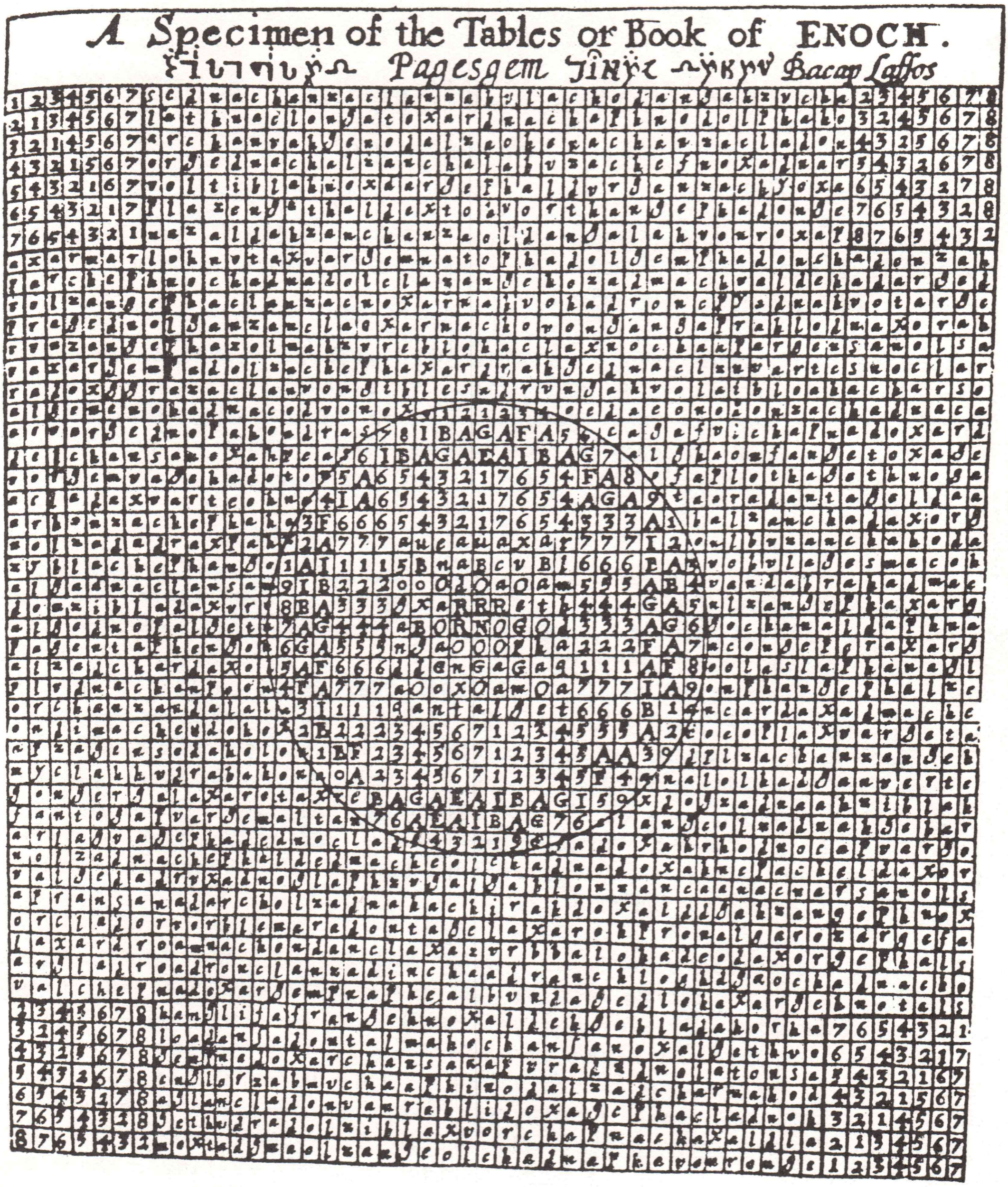
PHILIP M. ARNOLD

Shumaker, Wayne. Renaissance Curiosa. 1982. Medieval and Renaissance Text and Studies, State University of New York, Binghamton NY 13901. 208 pages. $15.00 cloth.

This book contains four essays in which the author, Professor Emeritus of English of the University of California at Berkeley, discusses four very different Renaissance writings, generally known only to specialists; all but one are in Latin, making them inaccessible to most people today. Shumaker's objective was to illustrate "the variety and unexpectedness of Renaissance thoughtways".

The first essay concerns A True and Faithful Relation of what passed for many Yeers between Dr. John Dee . . . and some Spirits, which ostensibly reports conversations between Dee and spirits, both good and evil, reached through "skryers" who gazed into crystal plates or balls. It was written in the 1580s by Dee, an Elizabethan polymath (1527-1608), but first published in 1659 by Meric Casaubon, an unfriendly editor. Shumaker gives biographical information on Dee, including discussion of his works in relation to Hermetism and Neoplatonism, and provides examples of the spiritual conversations, along with the reputed circumstances of their recording. He argues that Dee really believed that he talked with angels and devils, and that point of view has been taken by the majority of commentators on Dee [1]. There is, however, a minority with a different opinion.

Dee was well acquainted with Queen Elizabeth I and with Sir Francis Walsingham, head of her intelligence service. He travelled extensively in Europe and visited the Holy Roman Emperor Maximilian II and his successor Rudolph II as well as other rulers. He seems to have been sent on secret missions for either diplomacy or espionage, and a few writers believe that the conversations with spirits are really cryptograms [2]. Dee is known to have acquired a copy of the Steganographia of Trithemius for Elizabeth's minister Cecil and to have copied it. In Enoch his Book, another of Dee's writings, there are 49 diagrams, each containing 49 by 49 cells filled with letters and numbers, that look as if they might be encipherment tables (Figure 1). Dee also used what he called the Enochian alphabet, consisting of 21 letter-like symbols [3].



A Specimen of the Tables or Book of ENOCH.

Pagesgem Bacap Laffos

Figure 1. Table from Dee's Enoch his Book.

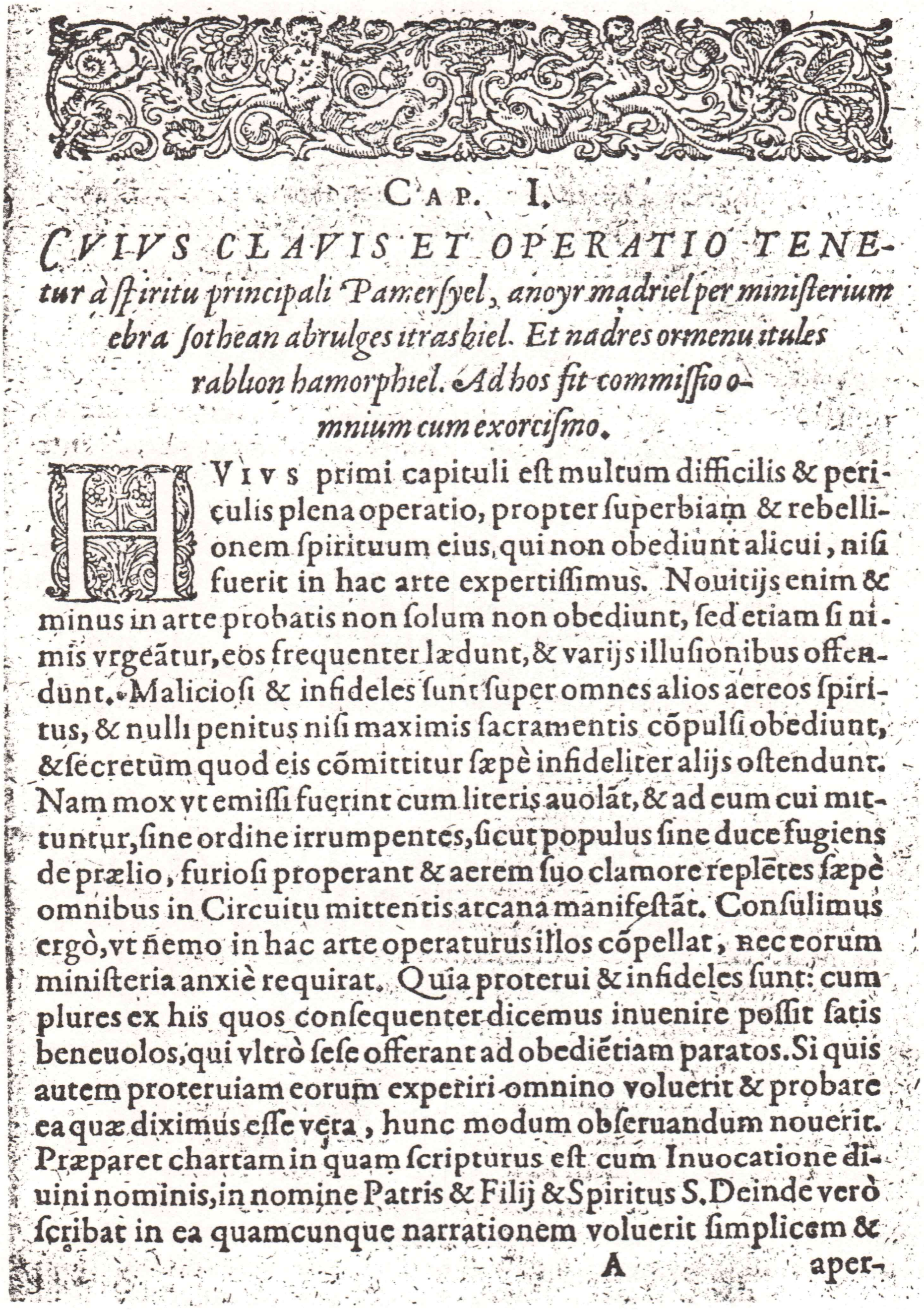
The first person to assert that cryptography was involved was Robert Hooke (1635-1703), long the secretary of the Royal Society. He wrote, "... I do conceive that the greatest part of the said Book, especially that which relates to the Spirits and Apparitions, together with their Names, Speeches, Shews, Noises, Clothing, Actions, and the Prayers and Doxologies, etc., are all Cryptographical ...[T]he Method and Manner thereof is so like to that of Trithemius his Cryptography, that I conceive (were it worth while) it would not be difficult to decipher a great part of it, by analogy thereunto." [4] However, no one seems to have taken up the challenge.

Shumaker's second essay is on a horoscope of Christ that was appended to the Lyon, 1555, edition of Girolamo Cardano's commentary on a work of Ptolemy on astrology. Cardano wrote on cryptography, but while the horoscope is a curious item, it has no connection with cryptography, so it need not be discussed here, except to say that the diagrams (Shumaker, page 71) used in casting horoscopes were used for cryptographic purposes during the Renaissance.

The third essay deals mainly with the Steganographia and the Polygraphia of Trithemius in conjunction with the Cryptomenytices et cryptographiae of Gustavus Selenus (Duke August of Braunschweig-Lüneburg). Among those who know Trithemius and his work by reputation, a minority will have actually examined the books, and still fewer will have made any attempt to decipher the cryptograms in them. This essay is an easy introduction to those daunting Latin texts.

Shumaker sketches Trithemius' life (based on Klaus Arnold's book [5]), including mention of his noncryptographic writings. He reviews the history of the Steganographia and the Polygraphia and points out that, despite Trithemius' protests and the explanations of authors like Selenus, Heidel, Schott, and others, the Steganographia has usually been seen as a treatise on black magic, and that even today there are eminent scholars like Frances A. Yates who have thought that the Steganographia is about magic rather than cryptography. Shumaker quotes Trithemius (from Polygraphia), "I have no commerce with daemons, never had any, and with God's protection will never have any; no studies in magic, necromancy, or the profane arts." Apparently the format involving invocations of spirits used by Trithemius arose from a desire on his part to mystify the public, but instead of awe and reverence, his book inspired fear and rejection.

Using examples from Selenus, Shumaker shows the principles underlying the cryptograms in the Steganographia (Figure 2). His explanations are simpler, more detailed, and more extensive than those given in other easily accessible books. Book III of the Steganographia was not finished and was not explained



CAP. I.

CVIVS CLAVIS ET OPERATIO TENEtur à ſtiritu principali Pamerſyel, anoyr madriel per miniſterium ebra ſothean abrulges itrasbiel. Et nadres ormenu itules rablion hamorphiel. Ad hos fit commiſſio omnium cum exorciſmo.

HVIVS primi capituli eſt multum difficilis & periculis plena operatio, propter ſuperbiam & rebellionem ſpirituum eius, qui non obediunt alicui, niſi fuerit in hac arte expertiſſimus. Nouitijs enim & minus in arte probatis non ſolum non obediunt, ſed etiam ſi nimis vrgeãtur, eos frequenter lædunt, & varijs illuſionibus offendunt. Malicioſi & infideles ſunt ſuper omnes alios aereos ſpiritus, & nulli penitus niſi maximis ſacramentis cõpulſi obediunt, & ſecretum quod eis cõmittitur ſæpè infideliter alijs oſtendunt. Nam mox vt emiſſi fuerint cum literis auolãt, & ad eum cui mittuntur, ſine ordine irrumpentes, ſicut populus ſine duce fugiens de prælio, furioſi properant & aerem ſuo clamore replẽtes ſæpè omnibus in Circuitu mittentis arcana manifeſtãt. Conſulimus ergò, vt ñemo in hac arte operaturus illos cõpellat, nec eorum miniſteria anxiè requirat. Quia proterui & infideles ſunt: cum plures ex his quos conſequenter dicemus inuenire poſſit ſatis beneuolos, qui vltrò ſeſe offerant ad obediẽtiam paratos. Si quis autem proteruiam eorum experiri omnino voluerit & probare ea quæ diximus eſſe vera, hunc modum obſeruandum nouerit. Præparet chartam in quam ſcripturus eſt cum Inuocatione diuini nominis, in nomine Patris & Filij & Spiritus S. Deinde verò ſcribat in ea quamcunque narrationem voluerit ſimplicem &

A aperby Selenus. It has often been regarded as a treatise on magic even by those who acknowledge the cryptographic nature of Books I and II. Shumaker argues that there is no sound justification for believing that the subject of Book III differs from that of the first two books. The *Polygraphia* is not controversial; it is more easily understood and there has never been any serious argument about its contents.

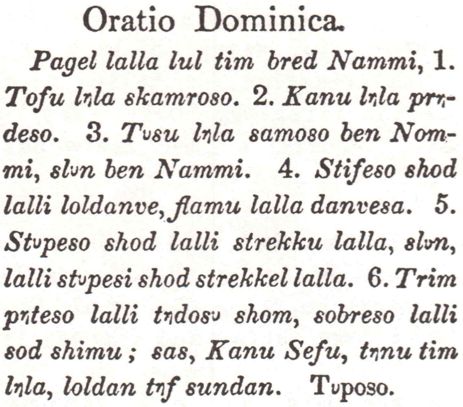
Toward the end of this essay Shumaker writes about Giovanni Batista Porta's *De furtivis literarum notis* and Blaise de Vigenère's *Traicte des chiffres*, but his treatment does not contain anything that would be newsworthy to readers of *Cryptologia*. He reproduces some tables and figures from those works.

The last essay is on George Dalgarno's *Ars signorum* (The Art of Signs), an early work on artificial language, published in 1661. To a person unacquainted with it, an artificial language represents a complex code system, just as various Indian languages did when used for military purposes during both World Wars. Shumaker reminds us that Bishop John Wilkins followed his book on cryptography with one on an artificial language and that tables in Trithemius' *Polygraphia* and Kircher's *Polygraphia nova et universalis* are a step on the way to an artificial language. In the latter book there is a section headed *Linguarum omnium ad unam reductio* (A reduction of all languages to one), which verges on a cryptographic system.

Dalgarno worked out his language thoroughly, and Shumaker describes it extensively, giving explanations and translations of examples that Dalgarno did not translate in the book. He includes a reproduction of 15 pages from Dalgarno's work for those interested in studying the language further. Figure 3 shows what the Lord's Prayer looks like in the language.

In all, Shumaker's book is a tour de force. To write it he had not only to call on his existing knowledge of languages, philosophy, and Renaissance thought, but also had to develop acquaintance with mathematical astrology and cryptology, as well as to learn Dalgarno's artificial language. Few persons would have the competence, interest, and patience to work through the recondite books he treats and to discuss them as he has -- thoroughly and informatively, without being pedantic.

(opposite) Figure 2. First page of Chapter I of Trithemius' *Steganographia*. *Pamersyel* identifies the cryptographic system. By taking alternate letters of the non-Latin words (i.e. omit *per ministerium* and *et*) the key to the system is given in a mixture of old German and Latin: *nym die ersten bugstaben de omni uerbo*. (Take the first letters of all words.) The printed text has two errors that can be corrected from manuscripts: *madriel* should be *madrisel*, and *rablion* should be *rablon*.



Oratio Dominica.

Pagel lalla lul tim bred Nammi, 1. *Tofu lηla skamroso.* 2. *Kanu lηla prηdeso.* 3. *Tυsu lηla samoso ben Nommi, slυn ben Nammi.* 4. *Stifeso shod lalli loldanve, flamu lalla danvesa.* 5. *Stυpeso shod lalli strekku lalla, slυn, lalli stυpesi shod strekkel lalla.* 6. *Trim pηteso lalli tηdosυ shom, sobreso lalli sod shimu ; sas, Kanu Sefu, tηnu tim lηla, loldan tηf sundan.* Tυposo.

Figure 3. The Lord's Prayer in Dalgarno's artificial language.

REFERENCES

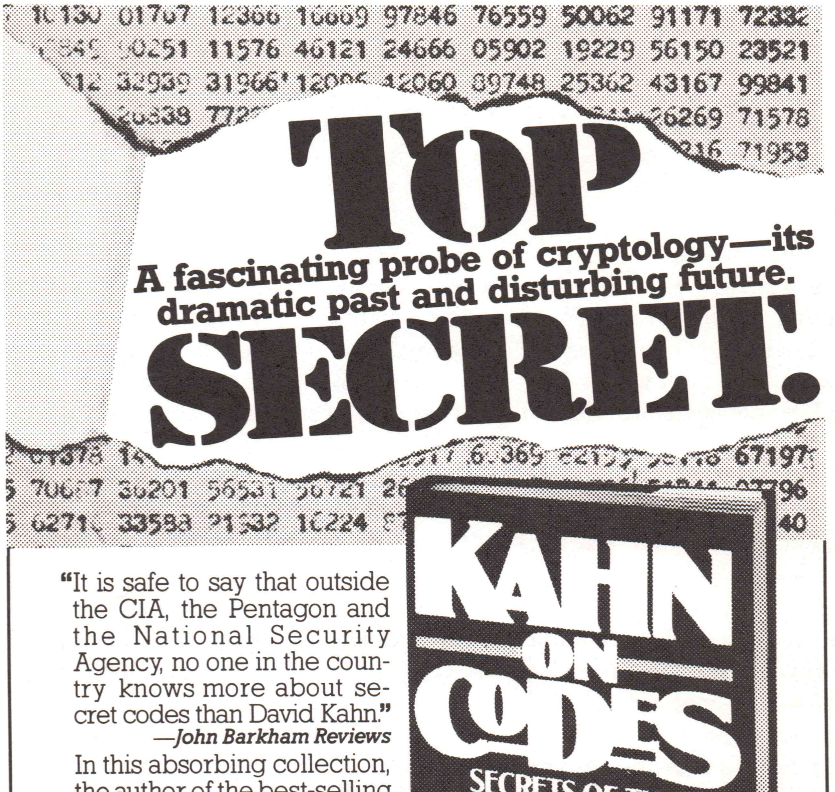
1. French, Peter J. *John Dee, The World of an Elizabethan Magus.* London, 1972. This work contains a good bibliography on Dee.

2. Deacon, Richard. *John Dee, Scientist, Geographer, Astrologer, and Secret Agent to Elizabeth I.* London, 1968. This book presents arguments that the conversations with spirits were cryptograms.

3. Deacon, op. cit. The plate facing page 230 shows the Enochian alphabet.

4. Hooke, Robert. *The Posthumous Works.* London, 1705. (Facsimile reprint, London, 1971.) Pages 206-207.

5. Arnold, Klaus. *Johannes Trithemius (1462-1516).* Würzburg, 1971.


TOP
A fascinating probe of cryptology—its dramatic past and disturbing future.
SECRET.
KAHN ON CODES
SECRETS OF THE NEW CRYPTOLOGY
BY THE AUTHOR OF THE BESTSELLING THE CODEBREAKERS
DAVID KAHN

REFLECTIONS ON THE "STATE OF THE ART"

C.A. DEAVOURS

I write this article at the risk of revealing myself to be a stick-in-the-mud. After 10 years of writing, researching, teaching, consulting, planning cryptographic systems and breaking other people's, and just talking to an awfully lot of people about Cryptology, I find myself somewhat at odds with the conventional wisdom about the subject which permeates the media.

Day-to-day work in cryptography and cryptanalysis seems to me a lot different from what I read (even in technical journals) and the true situation in regard to what is happening and what is not in the field appears, from my viewpoint, distorted.

Perhaps the greatest fallacy about cryptology is about the impact of computers on the subject. The type of statements to which I object usually go something like this:

> With the advent of computers, the subject of cryptanalysis became of academic interest only since the computer allows one to use algorithms of such exceedingly great complexity that they are, for all practical purposes, unbreakable. Low cost microprocessors have further amplified this trend, and now even the smallest of countries and businesses can have unbreakable codes and ciphers.
>
> Agencies like NSA are thus experiencing a "dim out" in high grade intelligence derived from codebreaking.

While there are some grains of truth in the above statement, it is, on the whole, quite misleading. One would think that the excessive claims and resulting embarrassment experienced by many advocates of public key cryptosystems over the last few years would have led to more caution on the part of those who write about matters cryptologic.

True enough, many nations have secure ciphers, and these ciphers are electronic. What else is new? For decades, secure cryptographic methods have been known and used. Computers have nothing to do with this fact. When a country failed to use cryptography well, the results could be disastrous. This is still true, and ciphers are still being broken every day. In reality, the transition to electronic methods has been accompanied by a lot of retrogression. This happened because most commercial designers of cryptographic equipment didn't have much knowledge about the subject and, further, didn't have anywhere to learn much about it. The same applies for most of the world's governments. Most nations have to believe what the machine salesman tells them about the security of the devices he sells. Second opinions are hard to come by. As far as cryptanalysis goes, less than a dozen nations outside the major powers show any serious interest in the subject.

Exotic cryptographic systems and codebreaking machinery are exciting to talk about, but one often loses sight of what we should be about here. After all, many nations of great political importance in the world don't even have a reliable source of electricity and an Apple II represents advanced computer technology. Cryptography is used primarily for privacy and, to a lesser extent, for authentication. If a 16th century nomenclator works as well as DES why not use it? You not only save a lot of money, but make yourself a lot less vulnerable to electronic eavesdropping. This last fact is of decisive importance in some situations. The trick is getting someone who can tell you what systems to use for your particular situation. The cryptanalytic caliber of private consultants generally leaves a lot to be desired.

I have often speculated as to why otherwise sensible people engage in the design and implementation of cryptographic systems when they have never had the least experience in the field of cryptanalysis. Let me go even further -- the majority of people engaged in this work today can't even solve problems that Friedman, Rowlett, et al, conquered 50 years ago. I'm not necessarily excluding myself form the above statements.

Being "state of the art" in cryptography is NOT a desirable situation. After all, electronic versions of many "old" systems and machines run a lot faster on microprocessors than most "modern" algorithms, and they have the advantage of having been around a long time and having a lot known about their strengths and weaknesses.

If one is truly serious about security and cost effectiveness, the above paragraph should be weighed heavily.

In spite of my earlier comments about the quality of public cryptographic and cryptanalytic work, I am a definite advocate of private algorithm design. In the end, it is the overall use of system which usually determines effectiveness much more than intrinsic cryptographic strength. To see this, one only need contemplate the large number of DES based EFT systems which have been broken and needed redesign because of the improper use of an otherwise adequate cipher. "Force fitting" someone else's black box or program to your application can't be expected to produce good results. If you start from the ground up and give your designers adequate information, the result is likely to be better even though the algorithms used may not match DES or public key methods in cleverness.

It has always troubled me that DES is called the "Data Encryption STANDARD." Cryptographers should avoid "standards" like the plague. If the history of cryptology teaches anything at all, it demonstrates this fact repeatedly. Why should private individuals want to adopt a standard cipher recipe when no sane government would do the same?

Some comments about NSA:

> As a child, I can remember running across the muddy fields of Fort Meade when construction began on the main building. (My father worked there.) Over the years, I have known many people who have worked at the Agency. That place is always changing. There seem to be cycles when NSA becomes more restrictive and obstructive in its dealings with the outside world and times when the reverse is true. This ever changing face occurs somewhat because of shifts in the Administration in Washington. More often, however, something is written or said in the media that causes bureaucratic embarrassment within the organization, or might even cause the Agency to lose out on a valuable source of intelligence. (I'm not talking about some country changing its ciphers.) When this happens, the word goes forth and the draw bridge over the moat is pulled up.
>
> I think that the Agency has always been much too restrictive in what information they chose to declassify. I can see the viewpoint of the other side, however; and were I on the inside looking out, I might well feel the same. In the end, it is to the interest of everyone that NSA does the best possible job in gathering and evaluating information since this will go farther towards preventing a nuclear war than all of the speeches and disarmament rallies which will ever be held. That's a personal opinion, of course.

CRYPTOLOGY AND THE LAW

LOUIS KRUH

Having received my J.D. degree recently, I thought it would be timely for a series of articles which review the laws, regulations and other governmental rules relating to cryptology.

Generally, passage of these laws, revisions or amendments aroused little interest. Their application, however, draws wide attention. For example, in 1977, when participants in an IEEE meeting were warned that open discussion of cryptologic advances could be a violation of the International Traffic in Arms Regulation (ITAR), there was a flurry of newspaper and journal articles. The Invention Secrecy Act was similarly highlighted when two attempts were made in 1978 to apply secrecy orders on patent applications for cryptographic items. (ITAR and invention secrecy will be discussed in future articles.)

Slightly more than 50 years ago, when the State Department learned that Herbert O. Yardley — who, a few years earlier, had written The American Black Chamber to their great consternation — had completed another manuscript which might contain more decoded dispatches, they quickly submitted a bill to Congress to prevent the publication of decoded messages sent by a foreign government. That law with some minor amendments is still in force today and will be the subject of a later column.

For this initial article on the subject we present the first attempt by Congress to protect military information. The bill, H.R. 26656, was passed March 3, 1911, and was titled, "An Act to prevent the disclosure of national defense secrets." While it does not include any specific mention of codes or ciphers, they presumably were covered by the reference to "documents."

CHAP. 226. — An Act To prevent the disclosure of national defense secrets.

March 3, 1911.
(H.R. 26656.)
(Public, No. 470.)
National defense.
Offenses specified.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That whoever, for the purpose of obtaining information respecting the national defense, to which he is not lawfully entitled, goes upon any vessel, or

Obtaining unlawful information.

Obtaining photographs, sketches, plans, etc.

Receiving unlawful information.

Communicating information.

Disclosing plans, etc.

enters any navy-yard, naval station, fort, battery, torpedo station, arsenal, camp, factory, building, office, or other place connected with the national defense, owned or constructed or in process of construction by the United States, or in the possession or under the control of the United States or any of its authorities or agents, and whether situated within the United States or in any place noncontiguous to but subject to the jurisdiction thereof; or whoever, when lawfully or unlawfully upon any vessel, or in or near any such place, without proper authority, obtains, takes, or makes, or attempts to obtain, take, or make, any document, sketch, photograph, photographic negative, plan, model, or knowledge of anything connected with the national defense to which he is not entitled; or whoever, without proper authority, receives or obtains, or undertakes or agrees to receive or obtain, from any person, any such document, sketch, photograph, photographic negative, plan, model, or knowledge, knowing the same to have been so obtained, taken, or made; or whoever, having possession of or control over any such document, sketch, photograph, photographic negative, plan, model, or knowledge, willfully and without proper authority, communicates or attempts to communicate the same to any person not entitled to receive it, or to whom the same ought not, in the interest of the national defense, be communicated at that time; or whoever, being lawfully intrusted with any such document, sketch, photograph, photographic negative, plan, model, or knowledge, willfully and in breach of his trust, so communicates or attempts to communicate the same, shall be fined not more than one thousand dollars, or imprisoned not more than one year, or both.

Punishment for communication to foreign governments, etc.

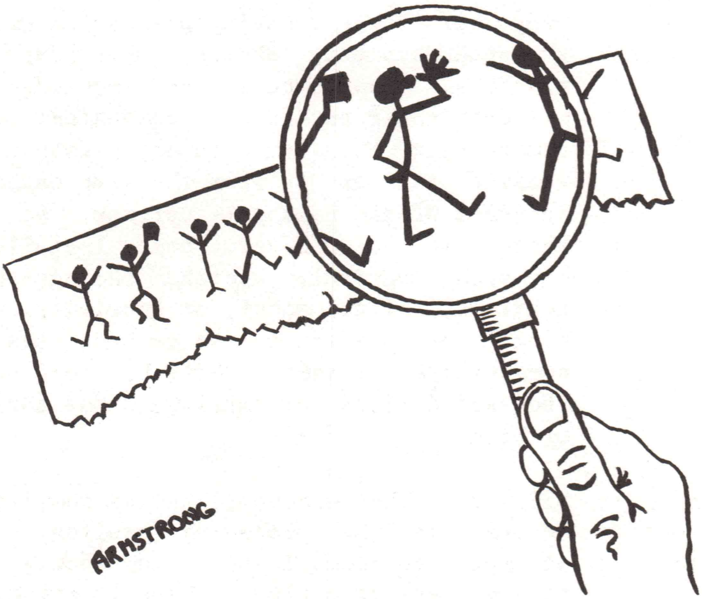
SEC. 2. That whoever, having committed any offense defined in the preceding section, communicates or attempts to communicate to any foreign government, or to any agent or employee thereof, any document, sketch, photograph, photographic negative, plan, model, or knowledge so obtained, taken, or made, or so intrusted to him, shall be imprisoned not more than ten years.

Jurisdiction for offenses on high seas.

In the Philippines.

SEC. 3. That offenses against the provisions of this Act committed upon the high seas or elsewhere outside of a judicial district shall be cognizable in the district where the offender is found or into which he is first brought; but offenses hereunder committed within the Philippine Islands shall be cognizable in any court of said islands having original jurisdiction of criminal cases, with the same right of appeal as is given in other criminal cases where imprisonment exceeding one year forms a part of the penalty; and jurisdiction is hereby conferred upon such courts for such purpose.

Approved, March 3, 1911.



"ARROGANT, HOLMES? HOW CAN YOU DEDUCE OUR QUARRY IS ARROGANT?"

CIPHER EQUIPMENT

LOUIS KRUH

This column presents a paper by Donald W. Davies of the UK National Physical Laboratory.

The machine he describes is somewhat complex but yet apparently simple in its output. Details are not available on the inventor, the date of his machine or what use was made of it. If any reader can furnish details it would be appreciated.

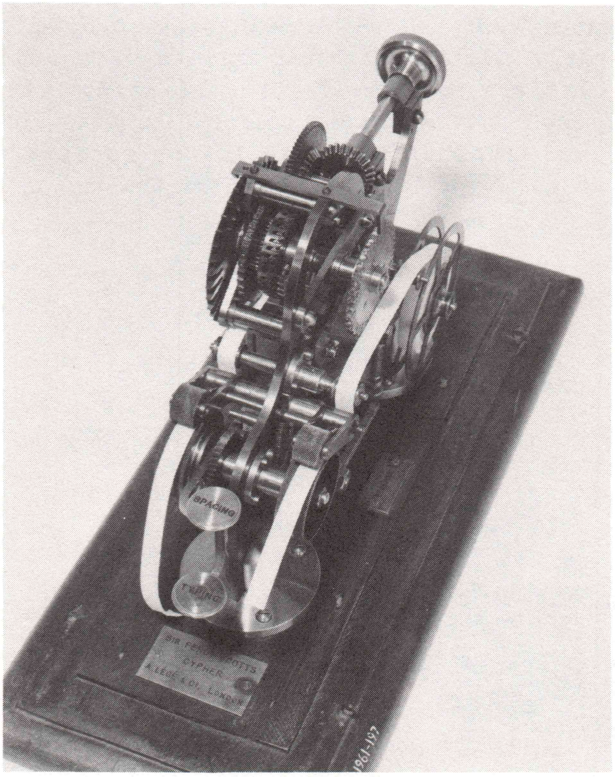


Figure 1. Sir Percy Scott's Cypher.

SIR PERCY SCOTT'S CYPHER

DONALD W. DAVIES

This machine, held at the Science Museum, is shown in the photographs. It is intended to produce two printed tapes showing plain and cipher text. An engraved label says 'Sir Percy Scott's Cypher' and below this 'A Lege' Co. London'. (See Figure 1.) Approximate overall dimensions are 320 x 200 (high) x 100 mm.

The mechanism is of heavy construction, mainly of brass. Its general style of design is like that of Babbage's machines - with heavy, elaborately machined parts. The two printing wheels are joined together by a coupling with 36 teeth. Each wheel has a written alphabet on its face and a corresponding alphabet in raised letters on its edge for printing. At one end of the machine is a control knob and two paper rolls. The other end has two large keys marked 'Space' and 'Type'. The control knob rotates the two coupled wheels together. When the 'Type' key is depressed the two

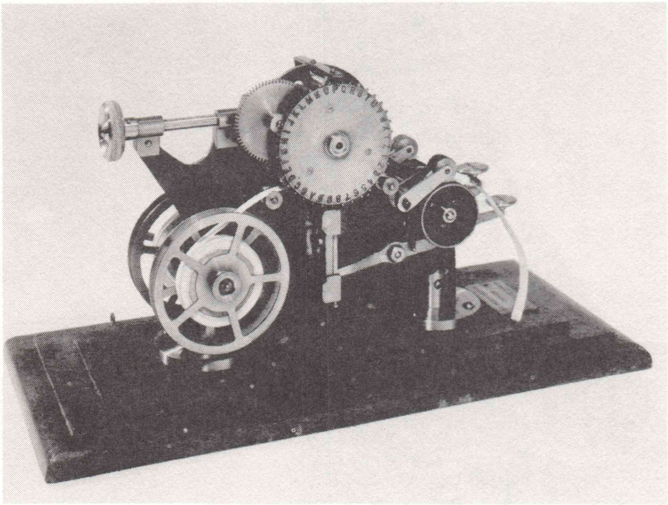


Figure 2.

wheels type and, as the key is released they move to a new position of the coupling, stepping one position relative to each other. Therefore their action is somewhat like that of the Wheatstone machine except that the alphabets are equal in size and the stepping is regularly once per character. When the 'Space' key is depressed, both paper tapes advance without printing. If this is intended for word spacing, it reveals word spaces in the ciphertext, but no instruction for use is available.

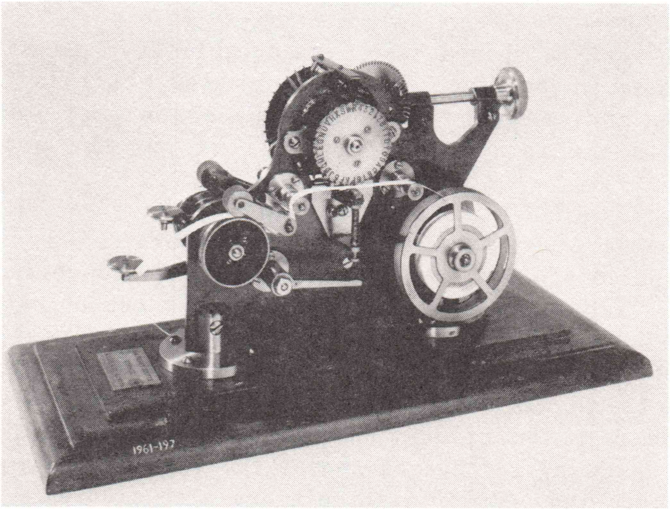


Figure 3.

Looking from the control knob end, (Figure 2) the right most wheel has the regular alphabet A-Z, 1 2 3 4 5 6 7 8 9 0, reading in clockwise order. Looking at the open face of the other wheel (Figure 3) the corresponding order is anti-clockwise and the alphabet reads:-

1 2 3 4 R W S X H V U N G E L M Q 0 J 5 F K P 6 7 8 C A 9 O Y D T I B Z

The 0 symbol is clearly the zero, but there is no way to distinguish 1 from I, except the presumption that 1234 are all numerals. Each time a character is printed, the permuted alphabet moves one place to its right, i.e. 1 takes the place of 2.

We surmise that encipherment is by turning the control knob to set the cleartext letter on the unpermuted wheel and reading the ciphertext from the other wheel, pressing the 'Type' key to record both on tape and, by so doing, move the permuted alphabet wheel forward one tooth.

The mechanism is fully operational. The only mechanical defects are corrosion or some other material on the permuted printing characters and lack of an inking mechanism. Instead of printing, the machine embosses the paper strip by pressing the tape on the type wheels by pieces of hard rubber. There is no sign of an inking mechanism. The embossing is rather spoilt by serrated drive wheels and is, in any case, not easily visible.

Any serious cipher machine should have a changeable key, usually the permuted alphabet in this kind of machine. But the permuted wheel is firmly fixed to its shaft by a pin and screws. This, and the absence of inking makes one think that what we see is a test piece to test out the mechanism, not a complete machine.

The relative stepping of the wheels is very elaborate. A rod moves up to enter one of 36 tapered slots in the unpermuted wheel, to correct its position and hold it firm. Two round pins in a collar move the coupling with its 36 teeth, together with the permuted print wheel out of engagement with the other wheel and press 36 teeth on the other side of the coupling against two groups of similar, fixed teeth. These teeth have sloping ends and are staggered, so that they turn the permuted print wheel half a step. Then the 'Type' key is released the main coupling re-engages and at the same time completes the one-tooth movement, since the ends of its teeth are also sloping.

The mechanism seems complex and expensive for what it achieves, and seems less effective than the simpler Wheatstone device, but it does have, in embryo, printing mechanisms for plaintext and cyphertext. A means for setting a key, for example by changing the permuted alphabet, would be essential for a serious machine.

A FURTHER WEAKNESS IN THE COMMON MODULUS PROTOCOL FOR THE RSA CRYPTOALGORITHM

JOHN M. DELAURENTIS

[This work performed at Sandia National Laboratories supported by the U.S. Department of Energy under contract number DE-AC04-76DP00789.]

A secure communications system -- based on the RSA cryptoalgorithm -- that has been reinvented several times would have a central keying authority (CKA) choose the secret pair of "good" primes p and q and then calculate pairs of encryption/decryption exponents, e_i and d_i for all the subscriber/users to the system. A user would receive a public list -- most likely in a PROM, containing the common modulus $M = pq$ and the public keys for all of the subscribers. He would also be issued his secret private key whose security would be both his responsibility and in his own interest. The merits of such a scheme are that both the key distribution and key management problems are greatly simplified, and that the required cryptographic calculations are the same for all users which could make it much easier for the provider of the secure communications service to supply equipment for the subscriber/users since all of the equipments could be identical.

Simmons [1] has recently shown that this protocol failed as a privacy channel if a message was ever encrypted and sent to two or more receivers, i.e., that an outsider (not a subscriber/user) using only the publicly exposed information could with unacceptably high probability decrypt the ciphers to recover the message. In this note we show that the common modulus protocol is even more vulnerable to attack by insiders (subscriber/user) who by using either a probabilistic or a deterministic method can "break" the cryptosystem; that is, an authorized user can decrypt ciphers intended for other recipients as well as being able to sign messages in undetectable forgeries of other users' signatures. First we demonstrate a probabilistic method suggested by Simmons for factoring the modulus; this factorization can then be used to compute encryption/decryption exponents. Next, we develop a deterministic algorithm, which computes encryption/decryption exponents without factoring the modulus.

Suppose A has entered his public key e_A into the public directory and that d_A is his secret decryption key. Similarly, let (e_B, d_B) be the pair of encryption/decryption exponents of another user B (e_B is also made public, but d_B is known only to B). The public keys serve the dual purpose of authentication if used to decrypt ciphers or of privacy if used to encrypt messages, i.e., e_A can either be used to authenticate ciphers sent by A or to encrypt messages into ciphers that only A can decrypt. First, we demonstrate how an insider (for example B) can, with high probability, factor the modulus. The approach we use is similar to the methods used in primality testing [2].

Let $e_Bd_B - 1 = 2^k\varphi$ where φ is odd and let a be a random integer in the interval $1 < a < M-1$. Assume that $(a,M) = 1$, otherwise the Euclidean algorithm can be applied to a and M to compute either p or q. Under the assumption that a is relatively prime to M, we develop a probabilistic method for factoring M.

Suppose we can compute a number $b \neq \pm 1 \bmod M$ such that

$$b^2 = 1 \pmod M \quad .$$

It is not difficult to see that this provides a factorization of M. To this end we define $c = b \bmod M$ where c lies in the range $1 < c < M-1$ and observe that

$$c^2 - 1 = 0 \bmod M$$

or

$$(c-1)(c+1) = 0 \bmod M \, .$$

The primes p and q cannot both divide c-1 or c+1, so the greatest common divisor of M and c-1 (or c+1) yields a factor of M. It follows that if we can quickly calculate a nontrivial square root of 1 (different from ± 1 mod M) then we can readily factor M. The following procedure provides, with high probability, a method of accomplishing this.

Since $e_Bd_B - 1 = 2^k\varphi$ is a multiple of Φ (M) we have

$$a^{2^k\varphi} = 1 \bmod (M) \quad .$$

Consequently, there exists a smallest nonnegative integer k′ such that

$$a^{2^{k'}\varphi} = 1 \bmod (M) \quad .$$

If $k' > 0$ and if $a^{2^{k'-1}\varphi} \neq -1 \bmod (M)$, then $b = a^{2^{k'-1}\varphi}$ is a nontrivial square root of 1. We show that this procedure fails at most half the time; actually, for most M it fails less frequently.

Let b_M represent the set on which the algorithm fails; that is, the set of units a such that

$$a^{\varphi} = 1 \pmod M$$

or

$$a^{2^t\varphi} = -1 \pmod M \text{ for some } t \text{ in } 0 \le t < n$$

The latter constraint can be modified slightly. Let $p - 1 = 2^i\alpha$ and $q - 1 = 2^j\beta$ where α and β are odd. We assume that $i \le j$. It is not difficult to show that for $t \ge i$, $a^{2^t\varphi} = 1 \bmod p$, consequently $a^{2^t\varphi} \ne -1 \bmod (M)$ for $t \ge i$. The set b_M can be redefined as the set of units a which satisfy

$$a^{\varphi} = 1 \pmod M$$

or (*)

$$a^{2^t\varphi} = -1 \pmod M \text{ for some } t \text{ in } 0 \le t < i.$$

Counting the number of solutions to these equations leads to the probability of failure.

To determine this probability, we will need the following observation. For any prime p and any integer r, the number of solutions to the congruence relation $a^r = 1 \pmod p$ is the number of solutions to $rs = 0 \pmod{p-1}$, namely $(r,p-1)$. This result is derived by replacing a with g^s where g is a primitive root and noticing that for $d = (r,p-1)$ the only solutions to $rs = 0[\bmod(p-1)]$ have the form

$$r \cdot t \cdot \frac{p-1}{d} = \frac{r}{d}t(p-1) = 0 \bmod (p-1)$$

for t in the range $0 \le t < d$.

We consider the first restriction in (*). From the preceding observation, the number of solutions to the congruence $a^{\varphi} = 1 \bmod p$ is $(\varphi,p-1) = (\varphi,\alpha) = \alpha$, (recall that $p - 1 = 2^i\alpha | 2^k\varphi$). By the Chinese remainder theorem the polynomial equation $a^{\varphi} = 1 \pmod M$ has $(\varphi,p-1)\ (\varphi,q-1) = (\varphi,\alpha)(\varphi,\beta) = \alpha\beta$ solutions.

The second of the restrictions in (*) implies that $a^{2^t\varphi} = -1 \pmod p$. Again, by the preceding observation we know that the equation

$$a^{2^{t+1}\varphi} = 1 \pmod p$$

has $(2^{t+1}\varphi,\ p-1) = 2^{t+1}\alpha$ solutions (recall that $t < i$). The solutions to the congruence

$$a^{2^t\varphi} = 1 \pmod p$$

accounts for $(2^t\varphi,\ p-1) = 2^t\alpha$ of them. The remaining $2^t\alpha$ solutions must be solutions of

$$a^{2^t\varphi} = -1 \pmod p\ .$$

According to the Chinese remainder theorem, the equation $a^{2^t\varphi} = -1 \pmod M$ must have $2^t\alpha \cdot 2^t\beta = 2^{2t}\alpha\beta$ solutions.

Summing over the number of solutions to each of these equations yields

$$b_M = \alpha\beta\left(1 + \sum_{t=0}^{i-1} 2^{2t}\right)$$

Since the number of elements in the multiplicative group modulo M is equal to $(p-1)(q-1) = 2^{i+j}\alpha\beta$, the probability of a failure is given by

$$\left(1 + \sum_{t=0}^{i-1} 2^{2t}\right)/2^{i+j} = [1+(4^i-1)\ /\ 3]\ /\ 2^{i+j}\ .$$

This probability is bounded above by 1/2 since

$$[1 + (2^{2i}-1)/3]\ /\ 2^{i+j} = (2^{1-i-j}+2^{i-j})/3 \le \left(1/2 + 1\right)/3 \ = 1/2$$

where the inequality follows from the observations $1 \le j$, $1 \le i$, and $i \le j$. It follows that, with probability at least 1/2, the factors of M are obtained. In other words, the expected number of trials until success is no greater than 2.

If one assumes the extended Riemann Hypothesis then for some positive constant c there exists $a \leq c(\text{tn } M)^2$ such that either $(a,M) \neq 1$ or a satisfies the preceding algorithm [2]. Thus, we would have a deterministic method for factoring M in $O[(\log M)^3]$ multiplications as opposed to a probabilistic method requiring on the average $O(\log M)$ multiplications.

It is interesting to observe that it is possible for an insider to decrypt intercepted ciphertext messages as well as being able to sign messages without actually factoring the modulus. Although this procedure does not provide a factorization of M, it is a deterministic algorithm; and the analysis of its running time does not assume the extended Riemann Hypothesis.

Without knowledge of d_A or $\Phi(M)$, it is possible for B to construct an inverse for e_A. By definition of e_A, e_B, and d_B, we have

$$(e_A, \Phi(M)) = 1$$

and

$$e_B d_B - 1 = k\Phi(M) \qquad k \varepsilon Z^+ \quad ,$$

$\Phi(M)$ is the Euler phi function. Dividing $e_B d_B - 1$ by any factors which it has in common with e_A leads to the quotient $n \equiv (e_B d_B - 1)/f$ which is relatively prime to e_A that is

$$(n, e_A) = [(e_B d_B - 1)/f, e_A] = 1,$$

where f consists of (possibly) powers of the common divisors of $e_B d_B - 1$ and e_A.

The computational difficulty of computing f is at worst $O[(\log M)^2]$. Let

$$(e_B d_B - 1, e_A) = (n_0, e_A) = h_0 \ .$$

f is found by successively applying the Euclidean algorithm to

$$(n_i, e_A) = h_i$$

where $n_i = (n_{i-1}) \ / \ (h_{i-1})$. This iterative procedure terminates when $h_i = 1$ for some i, at which point $f = \prod_{j=1}^{i} h_j$ and $n = n_i$. Either the procedure terminates at step i, or else $h_i \geq 2$, i.e., $2n_i \leq n_{i-1}$, hence at most $O[\log(e_B d_B - 1)] \approx O(\log M)$ are needed — each of which requires the execution of the Euclidean Algorithm which is also of $O(\log M)$ difficulty.

Notice that the divisor f is relatively prime to $\Phi(M)$ since e_A was chosen to be relatively prime to $\Phi(M)$. Since

$$n = (e_B d_B - 1)/f = (k/f)\ \Phi(M) \quad ,$$

it follows that f divides k, so that n is a multiple of $\Phi(M)$. We have constructed an integer n which is both relatively prime to e_A and a multiple of $\Phi(M)$. An application of the Euclidean algorithm yields

$$an + be_A = 1 \quad ,$$

where b can be forced to be positive, i.e., $b \varepsilon Z^+$. Since n is a multiple of $\Phi(M)$ we conclude that

$$be_A = 1 - an = 1 \bmod \Phi(M) \quad ,$$

that is, b is congruent to d_A mod $\Phi(M)$.

If the message m is encrypted with the exponent e_A to form the cipher c

$$m^{e_A} = c \ (\mathrm{mod}\ M) \quad ,$$

m can be recovered by B as follows

$$C^b = m^{be_A} = m \bmod (M) \quad ,$$

so that B can decrypt any intercepted ciphertext message.

Similarly if B "signs" the message m with the exponent b to form the "signature"

$$m^b = c \bmod (M) \quad ,$$

then to determine the authenticity of this "signature" an observer would use A's public key as follows:

$$c^{e_A} = m^{be_A} = m \ (\mathrm{mod}\ M) \quad .$$

As claimed, B has successfully forged A's signature to the message m.

Without knowing $\Phi(M)$ it is possible for any user to decrypt another subscriber's ciphertext messages and to forge his signature to an arbitrary message. In fact, any authorized user can construct a list of keys equivalent to the other subscriber's private keys.

Whichever method is used, it is clear that the common modulus RSA cryptosystem is totally insecure against deception by insiders. If a system must be protected against deceit by authorized users then it is not sufficient to simply distribute encryption/decryption pairs of exponents. As we have seen, knowledge of a single encryption/decryption pair is equivalent to factoring the modulus M.

REFERENCES

1. Simmons, G. J. 1983. A 'Weak' Privacy Protocol Using the RSA Cryptoalgorithm. Cryptologia. 7: 180-182.

2. Miller, G. L. 1976. Riemann's Hypothesis and Tests for Primality. Journal of Computer and System Sciences. 13: 300-317.

3. Rivest, R., A. Shamir, L. Adleman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Comm. ACM. 21: 120-126.

LETTER TO THE EDITOR

Dear Editor:

A reader of my Lucifer article [LUCIFER, A Cryptographic Algorithm. January 1984. Cryptologia: 22-42] pointed out that there is an inconsistency between the way I numbered the message bits in the Fortran code and the way they are numbered in the comments and drawings.

In the comments and drawings it appears that I numbered the bits so that 0 is the leftmost bit and 7 is the rightmost bit. Hence, bits 0-3 are the high order hexdigit and bits 4-7 are the low order hexdigit. This numbering corresponds to my interpretation of the APL program in the IBM Lucifer report [1].

On the other hand, in the Fortran Lucifer subroutine, I numbered the bits differently. The Fortran appears to be inconsistent with the original implementation. A correction appears below.

Correction to Lucifer subroutine:

replace lines 08100-08200 with

```
08100        do 400 kk = 4,7,1
08200          l = l*2+m(kk,jj,h1)
```

replace lines 08500-08600 with:

```
08500        do 410 kk = 0,3,1
08600          h = h*2+m(kk,jj,h1)
```

replace line 09100 with:

```
09100  v=(s1(l)+16*s0(h))*(1-k(jj,ks)+(s1(h)+16*s0(l))*k(jj,ks))
```

replace line 09800 with:

```
09800        tr(7-kk) = mod(v,2)
```

I hope that this correction will resolve the discrepancy between the Fortran and the text and comments.

Two additional corrections are fairly minor.

In Appendix 2 of the paper, there is a mistake in the listing of the main program that calls the Lucifer subroutine. Line 0800 needs to be corrected to the following:

```
0800 equivalence (k(0,0),key(0)),(m(0,0,0),message(0))
```

This was simply a typo.

The second correction is in the article itself. In discussing the transform-control-byte, the article states that the bits are accessed starting with bit 7 and ending with bit 0. Because of the above changes to make the bit numbering consistent throughout the article, diagrams, and Fortran programs, the text should state that the transform-control-byte is accessed starting with bit 0. This change makes the text consistent with everything else.

These problems arose because in the IBM Lucifer report, bits are numbered so that bit 7 is the high order bit in a byte. For ease of programming, it seemed more natural to have bit 0 be the high order bit, and I tried to make this change. Unfortunately, there seem to have been some places where I was not consistent. I believe that this problem is now corrected.

In closing, I would like to pass along a comment made by David Chaum of UC, Santa Barbara. He noted that the transform-control-bit depends solely upon the key, while in DES, the equivalent bits depends both upon the key and message. He suggested adding an autokeying feature to Lucifer by exclusive-or-ing together the bits of the byte being input to the S-boxes. The resulting bit is then exclusive-or-ed with the transform-control-bit derived from the key, and the bit that results, which now depends on both the key and the message, is used for transform control instead of the original transform-control-bit. This change would make the cipher stronger.

REFERENCE

1. Smith, J.L. 1971. The Design of Lucifer, A Cryptographic Device for Data Communications. IBM Research Report RC3326, Yorktown Heights, NY.

Dr. Arthur Sorkin, Computing Research Group, Lawrence Livermore National Laboratory, University of California, P.O. Box 808 Livermore, CA 94550 USA.

THE RESURRECTION OF MULTIPLE-KEY CIPHERS

JOHN M. CARROLL

INTRODUCTION

Multiple-key ciphers have at least three attractive properties:

1. They can be used to divide a secure communications network into compartments.

2. They can control the sharing of information in files. For example, access to relational databases could simultaneously be controlled with respect both to (a) security clearance/classification and (b) need-to-know.

3. They can strengthen existing cipher systems.

Multiple-key ciphering is not the same as multiple encipherment. In multiple encipherment, the transformation is:

$$C = f(K2(fK1,P))$$

In multiple-key encipherment, the transformation is:

$$C = f(K2,K1,P)$$

The essential difference is that in multiple-key encipherment the keys must be inserted simultaneously while in multiple encipherment they can be inserted at different times and in different places. Both techniques have unique advantages in different applications.

As an example of how multiple-key encipherment can be used to compartmentize communications, recall the Henry multiple-rotor electric coding machine (ECM) of World War II. One "key" was the "basket" or set of 10 rotors, a second key was the settings of the first five rotors, and the third key was the settings of the last five rotors. The possession of the basket granted access to a crypto channel (fleet command, communications security, etc.). One set of rotor settings might have been associated with a level of clearance (top secret, secret, etc.); the other set might have been associated with a particular network, like the Marianas Island net.

MULTIPLE-KEY CIPHER DESIGN

The same principles can be adapted to computer cryptography. We shall let key K1 select random characters that are to be combined with the plain-text characters; this is what is done in most reciprocal ciphers (that is, ciphers that use the same key for enciphering and deciphering). We can regard K1 as the crypto key.

However, instead of combining the characters by a bit-wise addition without carrying (exclusive ORing), we shall use key K2 to select random characters that will determine which of several functions we shall use to combine random characters with plain-text characters. We can regard K2 as the function key.

The combining functions are actually randomized Vigènere squares. There is one square for every character in the alphabet from which K2 makes its selection. Each character selected by K2 specifies a Vigènere square that is used to combine one random character selected by K1 with one plain-text character.

If the alphabets have A letters, then the set of A Vigènere squares can be selected randomly from:

$$(A!-1)! / (A!-A-1)!$$

possibilities. The set of Vigènere squares can be regarded as a third "key."

IMPLEMENTATION

Keys K1 and K2 must produce repeatable (pseudo)random sequences. One of the best and cheapest ways to do this is by using two Data Encryption Standard (DES) chips, one to generate crypto characters and the other to generate function characters.

We arrange the chips in the Cipher Block Chaining mode [1, pp. 149-151]. In this discussion, the term "block" is used synonymously with the terms "crypto character" or "function-control character" to connote a bit string of uniform length. The output blocks from the K1 chip will be combined with blocks of plain text using the Vigènere squares selected by the output blocks from the K2 chip.

If we regard the plain text as simply a stream of bits, block length can be selected by the system designer. The block length determines the length A of the cipher alphabets. The longer the block, the more electronically programmable read-only memory (EPROM) chips will be needed to store the Vigènere squares. With longer blocks, the cipher will be stronger but the cipher machine will be more cumbersome.

We have simulated this technique on a personal computer using a block (i.e. character) length of four. As a consequence, we provided sixteen 16-character by 16-character randomized Vigènere tables. We used multiplicative-congruential pseudorandom-number generators instead of DES chips to produce the K1 and K2 bit streams. The plain text was coded into a 16-character phonetic alphabet in which 1 = A; 2 = B or P; 3 = C, S, or Z; 4 = D or T; 5 = E; 6 = F; 7 = G; 8 = H; 9 = I, J, or Y; 10 = K, Q, or X; 11 = L; 12 = M; 13 = N; 14 = O; 15 = R; and 16 = U, V, W, or space; this was done for convenience in programming. However, irrespective of block length, once the plain text bit stream has been recovered, it can be interpreted in any desired format.

APPLICATIONS

1. Compartmenting Communications.

Using this multiple-key cipher, communications could be compartmentized by letting possession of the proper EPROM card permit access to a crypto channel (like the ECM "basket" did), using the function key to denote membership in a network, and using the crypto key as the station key for station-to-network-controller communications or as the session key for station-to-station communications.

2. Controlling Access to Data.

Much work remains to be done in devising models for controlled sharing of information by allocation of cryptographic keys. A simple application would be a relational database in which access to attributes (columns) was governed by need-to-know (e.g. an attribute might be "salary"); while access to groups of tuples (rows) was governed by level of clearance (e.g. "top secret" = "≥ $50,000 a year"). Function keys could permit access to columns while crypto keys could permit access to groups of rows. Of course, a person having the highest clearance would have to possess all the crypto keys and as many function keys as there are attributes to which he has access.

3. Strengthening DES.

There is good reason to believe that existing crypto systems could benefit from strengthening. When DES was introduced in 1974, its supporters estimated a useful lifetime of five years. Advances in computer hardware, especially in parallel processors and optical disk memories, make the prospect of attacking it more attractive than ever [1, pp. 97-101]. Moreover, a healthy skepticism exists regarding "public" key ciphers because of the reported breaking of the knapsack algorithm [2, p. 88], and because of recently announced advances in the factoring of large numbers [3]. The use of DES in a multiple-key cipher would produce a strong system indeed, especially if the plain text were first processed by a text-compression algorithm that does not transmit its dictionary. Even if the cipher were adopted primarily to strengthen DES, its multiple-key feature could be exercised to offer a time-dependent (i.e. key-of-the-day) option, while the EPROM boards could be utilized as a terminal signature mechanism whose authenticity could be accorded much more credence than the "here is" chip.

ACKNOWLEDGEMENT

The author thanks his colleague, Professor Helmut Juergensen, formerly of Darmstadt University, for many helpful suggestions and criticism.

REFERENCES

1. Demming, D. E. R. 1982. Cryptography and Data Security. Reading MA: Addison-Wesley. pp. 149-151.

2. Opening the "Trapdoor Knapsack." 1982. Time. (October 25, 1982.)

3. Cracking a Record Number. 1984. Time. (February 13, 1984.)

AAAS CRYPTO SESSIONS PROCEEDINGS: REVIEW

G. R. BLAKLEY

[Reprinted from SIAM REVIEW, Vol. 26, No. 1, January 1984. Copyright G. R. Blakley. Reprinted by permission.]

Secure Communication and Asymmetric Cryptosystems. Edited by Gustavus J. Simmons, Westview Press, Boulder, CO 1982. X + 338 pp. $30.00. ISBN 0-86531-338-5.

Occasionally a symposium works out well because the organizer strikes a tone which the participants sustain. G. J. Simmons organized a symposium in conjunction with the 1980 AAAS National Annual Meeting in San Francisco. The volume under review contains a record of some of that symposium, and it does sustain a tone. The authors are all well-known contributors to the cryptographic literature. The papers are all short and readable. In fact, every contributor keeps in mind the interested scientist, engineer or businessman at all times, even when presenting new research results. High school computer buffs well grounded in math could even get a good bit out of it.

Part 2 consists of papers 6-10, reprints of classic of the new cryptography. These were all, of course, in print before the symposium took place. Paper 6, "New Directions in Cryptography," by W. Diffie and M. E. Hellman, appeared in 1976. It is seminal and exciting. One of its claims to fame is that it introduced the notion of public key cryptosystem at a time when no examples were known to the public, though perhaps [KA82] NSA knew of possible implementations of the concept. "New Directions" stimulated an immense amount of subsequent work. Paper 7 is "Secure Communications over Insecure Channels," by R. Merkle, published in 1978. It took up the question of how to exchange information over public channels in such a way that the two communicating parties wind up in possession of a common cryptographic key unknown to any eavesdropper. "Secure Communications" led to a great deal of work on key exchange. Paper 8 is "Hiding Information and Signatures in Trapdoor Knapsacks," by Merkle and Hellman. It was published in 1978, and describes one of the two earliest and most famous publicly known public key cryptosystem (what

Simmons calls asymmetric cryptosystems and others call two-key cryptosystems). The Trapdoor Knapsack public key cryptosystems can be implemented at high speed and uses very large keys. In 1982 certain weaknesses [SH82] began to show up. Paper 9, also published in 1978, is "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" by R. Rivest, A. Shamir and L. Adleman. This paper describes the RSA public key cryptosystem. RSA cannot transmit information as fast as Trapdoor Knapsack, but the encoding process is a one-to-one onto function which makes it the vehicle of choice for digital signatures. No significant weaknesses of RSA, used only as a cryptosystem, have yet surfaced. But one must exercise extreme caution [DA82] when using it to sign messages under some circumstances. Paper 10 is "Symmetric and Asymmetric Encryption" by Simmons. It appeared in 1979, and is longer (almost 60 pages) and more demanding than the other papers in this volume. Where papers 6-9 announced inventions, or their imminence, this is a survey. Simmons takes pains, on pp. 277 and 289, to warn the unwary that overblown claims in Scientific America and Science for security of public key cryptosystems are not justified by present public knowledge. He does not claim that they are less secure than conventional cryptosystems either. He is perhaps too reticent in this. He was one of the first, if not the first, people to publicly suggest that public key cryptosystems might have to buy their desirable features at the cost of larger key size for a given security level than conventional cryptosystems. This possibility, recently referred to again [KA82], is a real one.

Part 1 consists of four papers actually presented at the symposium. A fifth symposium paper, Adleman's tutorial, is not included in the book. H.C. Williams starts off with an introduction to computational complexity and its uses and abuses in cryptography. He ends on a skeptical note struck by Simmons, I. Richards [RI82] and many others. Apart from the one-time pad, which has a key as long as the entirety of its message traffic, we don't really have any reliable assurances of cryptosystem security. Next comes another paper of Diffie's, drawing comparisons and contrasts between conventional and public key cryptosystems. It is illuminating and quite fair. There is one comment a casual reader of Diffie's paper should bear in mind. The Diffie-Hellman key exchange scheme was designed with GF(p) in mind, and has no known weaknesses. But attempts, such as the one mentioned on p. 50, to build GF(2^n) analogues of this scheme have been shown [HE80] to have some weaknesses. Next comes Merkle's paper on protocols for public key cryptosystems. This is a topic too often neglected. But public key cryptosystems are worthless without them as G.I. Davida [DA82] and others have recently reminded us. One could only wish that Merkle had written more. But at least his call for further work in this area has been heeded. Some of the most important uses of cryptography aren't much concerned with secrecy. In the last paper in Part 1, Simmons takes us on a quick guided tour of some such uses by exposing us to some real world authentication problems. The paper is short, but it can serve as an introduction to much interesting current work.

Part 3 consists of a single paper in which Diffie has been persuaded to overcome his wonted diffidence and tackle the problem of making a fifteen-year forecast of cryptographic technology through 1995. It is thoughtful, wide-ranging and doesn't contain anything that needs disavowing at the three-year milepost. Most of us will disagree with something or other in it, which is one of the reasons why it is a pleasure to read.

So much for the parts. What about the book as a whole? The reviewer knows of just five mathematically substantial books on cryptography available to the general public. The volume under review is the least demanding and easiest to read of the five. For the interested scientist who doesn't work in the area, and just wants some glimpses of what's going on, it is clearly the first choice. By the same token a student, businessman or engineer who must decide whether to study or use cryptography should read it or dip into it. It does a masterful job of giving easy access to a few major discoveries and a few important trends. If it whets your appetite for the subject then go on to Beker/Piper [BE82], Denning [DE82], Konheim [KO81], or Meyer/Matyas [ME82].

REFERENCES

[BE82] H. Beker and F. Piper, "Cipher Systems: The Protection of Communications," Northwood Books, London.

[DA82] G.I. Davida, "Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem," Electrical Engineering/Computer Science Dept. preprint TR-CS-82-2, Univ. Wisconsin at Milwaukee, October 1982.

[DE82] D.E.R. Denning, "Cryptography and Data Security," Addison-Wesley, Reading, MA, 1982.

[HE80] M.E. Hellman, "On the difficulty of computing logarithms over GF(q^m)," Proc. 1980 IEEE Symposium on Security and Privacy, Long Beach, CA. 1980. p. 3.

[KA82] D. Kahn, "Expert says secret code found not secret enough," Newsday, Nov. 10, 1982, p. 13.

[KO81] A.G. Konheim, "Cryptography: A Primer," Wiley-Interscience, New York, 1981.

[ME82] C.H. Meyer and S.M. Matyas, "Cryptography: A New Dimension in Computer Data Security," Wiley-Interscience, New York, 1982.

[RI81] I. Richards, "The invisible prime factor," American Scientist, 70(1982),pp. 176-179.

[SH82] A. Shamir, "A polynomial time algorithm for breaking Merkle-Hellman cryptosystems" (extended abstract), Applied Mathematics Dept. Preprint, Weizmann Institute, April 20, 1982; see also Proceedings of Crypto '82.

bbaba aabaa aabab babbb aabab aabab babbb.
aaaba babba aabaa bbabb aabba babaa bbaba aabba.

CRYPTANALYSTS' CORNER

GREG MELLEN

Readers who solved the October 1983 problems before the January 1984 issue appeared, with its cover picture of the modified Wheatstone device, are to be admired. In retrospect I think that I gave too little information and should have included probable words.

With regard to solving the problems, the information available to the analyst is scant. He knows only that he is dealing with a nonperiodic substitution cipher of the World War I era (the latter being a "given" in the October column).

It is instructive if not always fruitful to determine if isomorphs are present. Readers who succeeded with the October problems in uncovering the isomorph on which solution depended were determined indeed. The isomorph begins in Problem 1, Group 1 and Problem 4, Group 15.

3B4BTYZ3JNRGM . . . D43EEA3MLTAIA
YIZIMUVYDCLKH . . . XZTBB3Y4FN3A3

When the two sequences are chained, the following alphabet is obtained:

3UQJDXGKP2WTMHSONC4ZVRLFEBIA

Decimating this alphabet at interval 19 yields the original keyword alphabet:

PACKINGBOXESDFHJLMQRTUVWYZ234

Since he does not have the encrypting device (or know for sure that a device was involved), the analyst must proceed with a series of trial assumptions. With luck, the following trial may occur early in the series and thereby end it. It is a minor variation of the method used to solve a "standard" Wheatstone cipher. [1] The description of the method in print makes it appear slow and awkward, as do so many descriptions of cryptanalytic procedures. In practice, the process moves along rather quickly.

Let two strips be made, one with the pt alphabet and the second one, double length, with the keyword ct alphabet repeated. In this instance, we are dealing with a 29-character ct alphabet and a 30-character-plus-space pt alphabet.

The analyst may suspect that the repeated letter at the beginning of each message is a keying element, but he has no way to determine its meaning. Hence let some arbitrary initial alignment of the two strips be chosen.

We will begin the solution of message 1 in the October column:

(V V) 3 $\underline{B}$ 4 $\underline{B}$ T Y Z 3 $\underline{J}$ $\underline{N}$ R $\underline{G}$ M W 3 $\underline{F}$ $\underline{A}$ Q . . .

The seven underscored letters are ones which occur earlier in the ct alphabet than their immediate predecessors in the message. These letters will be used as a signal to shift the ct alphabet slide one position left with respect to the pt alphabet slide, simulating the rotation of the 29-space ct disk around the 30-space pt disk. In the arbitrary initial alignment, the slides appear thus:

ct: PACKINGBOXESDFHJLMQRTUVWYZ2$\underline{3}$4
pt: ABCDEFGHIJKLMNOPQRSTU2VWXYZ$\underline{3}$4+ ["+" = space]

The first message letter, 3, is located on the ct slide, and its counterpart, 3, is read from the pt slide, giving the first character of our trial decipherment. Before deciphering the second message letter, B, we move the ct slide one position to the left:

ct: ACKING$\underline{B}$OXESDFHJLMQRTUVWYZ23$\underline{4}$P
pt: ABCDEF$\underline{G}$HIJKLMNOPQRSTU2VWXYZ$\underline{3}$4+

The ct B is transformed into trial decipherment G. In the same slide position, we can decipher 4 as 3, so that for the first three message letters we have 3 G 3.

Again shifting to accommodate the next ct letter, B, we see:

ct: CKING$\underline{B}$OXESDFHJLMQR$\underline{T}$UVW$\underline{YZ}$2$\underline{3}$4PA
pt: ABCDE$\underline{F}$GHIJKLMNOPQR$\underline{S}$TU2$\underline{VW}$X$\underline{Y}$Z34+

Five letters can be deciphered in this position, and the trial sequence is thus 3 G 3 F S V W Y.

When this process is continued for the first 15 ct letters, the trial decipherment appears:

```
3 G 3 F S V W Y M B P B M S V . . .
```

When one completes the full message by proceeding in this manner, a frequency count will show that the message has been reduced to quasi-monoalphabetic terms, and can be solved as a simple substitution, with plaintext ENEMY+ACTIVITY+OBSERVED+IN+VICINITY+OF+GREQN+SECTOR. . .

The "GREQN" in the above solution is not a typo but follows the standard Wheatstone practice of substituting a little-used letter for the second letter of all repeats.

Before we leave this solution, several further notes: In the above pt sequence, the 2 following the U instead of appearing after the Z as the analyst might normally assume. The reason stems from the encrypting device. As shown on the January 1984 cover, the umlaut-U follows the uninflected U; I replaced it with the numeral 2.

Had the cipher used the standard English alphabet, or any alphabet that is known beforehand, there is a faster method of solution than by frequency analysis. Of the possible initial alignments of the ct and pt strips—30 in this instance—one, the one used for encipherment, will yield plaintext and the other 29 a Caesar substitution of the plaintext.

By running down the pt alphabet, therefore, the original text can be recovered, as shown in the last column below:

```
3 4 + A B C D E . . .
G H I J K L M N
3 4 + A B C D E
F G H I J K L M
S T U 2 V W X Y
V W X Y Z 3 4 +      etc.
```

As for the January problems, I regret that a garble in a key place would have prevented the recovery of the plaintext. The solution follows in large part the steps outlined above. The complication mentioned in the January text is that the pt alphabet was mixed as well as the ct alphabet.

There is a lengthy isomorph in Problem 3, Group 1 and Problem 4, Group 2:

YJ4UXF2SHH43P . . . CUWBCHEOFBHIT
MVUGLKQ400RZ3 . . . XGIJXOC2KJOT3

When chained:

Y M B J V H O 2 Q E C X L S 4 U G P Z N D A W I T 3 R F K

and when decimated at interval 15:

J A C K P O T S B D E F G H I L M N Q R U V W X Y Z 2 3 4

This is the keyword ct alphabet. Unfortunately, it is not possible to get beyond this with the problem text as printed.

So with a firm resolve to improve my proofreading, I will continue on the subject of symmetry of position. In the January column, the patent symmetry of position of Vigenere and other standard alphabet ciphers was reviewed.

There are three major kinds of symmetry of position: External, internal and reciprocal. The terms refer to the relationships between the ct alphabets within the enciphering tableau and the pt alphabet defining the border of the tableau.

Symmetry which exists not only among the ct alphabets within the tableau but extends to the pt alphabet as well is called external symmetry. It is manifested by all periodic ciphers which use the same alphabet—standard, mixed or keyword—running in the same direction for both pt and ct. As an example, the short excerpt below is from a partially reconstructed tableau for a period-4 cipher which used the keyword alphabet:

M U S I C A L E B D F G H J K N O P Q R T V W X Y Z

However, the analyst does not yet know the keyword alphabet, and initially constructs the matrix using the standard alphabet as the external (0) alphabet. The numerals 1-4 designate the four shifts of the ct alphabet.

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
1	Q		P			X										C			N						G		1
2	V				X	M	U		R				O	A				D		F		G					2
3		L		E				F	U			C					O		M						W		3
4				G	D						O				Q	R		V								U	4
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0

In this tableau note the relationship $C_0/P_1 = P_0/C_1$. This may be read simply as "C is to P as P is to C," with the subscripts being a convenience here to highlight the relevant alphabets.

The reciprocity of C/P = P/C indicates that ct alphabet 1 is the "14th alphabet," analogous to the N alphabet of the Vigenere tableau. Thus for every X = Y, we have Y = X. We can add the reciprocals to the first ct alphabet of the tableau:

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
1	Q		P			X	$\underline{Y}$							$\underline{S}$		C	$\underline{A}$		N					$\underline{F}$	G		1
2	V				X	M	U		R				O	A				D		F		G					2
3		L		E				F	U			C					O		M						W		3
4				G	D						O				Q	R		V								U	4
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0

And since we are dealing with external symmetry we can use relationships in the external, pt, alphabet to derive new relationships in the internal, ct, alphabets. Consider, for example, $D_0/Z_0 = G_4/U_4$. This relationship is symmetrical with $D_0/\underline{Z}_2 = G_0/U_2$, giving us the value $Z_c = D_p$ in the second ct alphabet. Similarly:

$Z_0/E_0 = U_4/D_4$ hence: $Z_2/E_3 = U_2/\underline{D}_3$
and $D_0/Y_0 = E_3/W_3$ so $D_3/Y_1 = E_3/\underline{W}_1$

Next, $G_2/D_2 = V_0/R_0$ yields $G_0/D_3 = V_0/\underline{R}_3$
$G_0/E_0 = U_2/X_2$ giving $G_4/E_3 = U_4/\underline{X}_3$

At this point the tableau appears as follows:

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
1	Q		P	$\underline{W}$		X	$\underline{Y}$							$\underline{S}$		C	$\underline{A}$		N				$\underline{D}$	$\underline{F}$	G		1
2	V			$\underline{Z}$	X	M	U		R				O	A				D		F		G					2
3		L		E			$\underline{D}$	F	U			C					O		M			$\underline{R}$			W	$\underline{X}$	3
4				G	D						O				Q	R		V								U	4
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0

In the interest of not using more space, I will leave the development at this point. I will note however that there is at least one more relationship which can be added. The reader's attention is directed to the A_0/S_0 relationship, and then the alphabets 2/1.

To end this issue's column, here is a cryptogram by Warren T. McCready which appeared in the July-August 1983 issue of The Cryptogram. It is a period 8 cipher using the same keyword alphabet for both pt and ct. When the tip is placed, the partial tableau illustrated is obtained. The reader is invited to complete the tableau, and read the message which, incidentally, is in easy Spanish.

```
UKHCY TGYVH GWMFG BIENN OQPVO WKFUY GZLRF WXGXF
SENIY GLPBM HGVWF VOFWF WYGAS MFSAV OZUKW ZZZYF
BRFNT XSKKE YNTXX VLRJH GWYMU BUHUY JETRF GVGJR
OWMNV WRTUL KXBZY ZUGNI AVEVL MQVEQ GRAMF ZANNC
UKHCY TGYVG WPVZW ZOGLK XAXYU GRZAN NCUKK ZUWEP
RWBKX YITVI KKYYX V
```

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
1					U									L				T	O								1
2			B		R				W																		2
3				M				U										J	F								3
4	G				N										H												4
5								G								U											5
6	W		G																								6
7		R												Y	J												7
8							E	M				T		R													8
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0

REFERENCES

1. Friedman, W. F. 1918. Several Machine Ciphers and Methods for their Solution. Publication No. 20, Riverbank Laboratories, pp. 6-36. [Reprinted: Laguna Hills, CA: The Aegean Park Press. Vol. 2 in the Riverbank Publication Series. 1979.]

LETTER TO THE EDITOR

Dear Editor:

The article on the Delastelle cipher in the April 1983 (Volume 7, Number 1) issue of Cryptologia pp. 170-179 contains a few minor errors, and a major error regarding applicability, corrections for which follow:

p. 174, line 3: "rows" should be "columns"
p. 177, first transposition on bottom of page: L'^{-1} should be L^{-1}
p. 178, matrix C: bottom line should be SFBUO.

The practical motivation for the paper seemed to be that using C and D, say, for deciphering, when A and B were made of easily remembered sequences, made it hard to decipher quickly (or conversely, if C and D were normal sequences, and A and B were mixed).

In place of the above, we are given mixed sequences in A and B, granted to be reciprocal, but which make both enciphering and deciphering difficult. This accomplishes little more than substitute justice for practicality. A simple procedure corrects the problem.

Figure A is Figure 6 of the article, as corrected above. Figure B is an alphabet containing the sequence used in matrix A of Figure 6 as its upper component, and the normal sequence (without J) as the lower one. Use this pair to encipher the elements of matrices C and A. Figure C is another alphabet such as Figure B, but using the sequence of matrix B of Figure 6. Use this to encipher matrices D and B.

Figure D is the new set of 4 matrices. It has the reciprocal property, and is easy to use.

Observe that there are 26! choices for each of A and B, according to taste, including the two in the article, but 26! minus epsilon are of no interest to the poor cryptographic clerk.

```
A:  W P I C Q     C:  R L K T A
    F B O S U         D X E Z M
    L K A R T         C W P Q I
    G N V Y H         Y G N H V
    X E M D Z         M I T C Z
```

For American use, as opposed to French (which uses W rarely), W is substituted for J. Caps are used throughout for ease of reading.

```
D:  P V F U K     B:  U P V K F
    E R N O G         W Q A X D
    Q A D W X         O E R G N
    I T Z M C         B L S H Y
    L S Y B H         M I T C Z
```

Figure A

```
W P I C Q F B O S U L K A R T G N V Y H X E M D Z
A B C D E F G H I K L M N O P Q R S T U V W X Y Z
```

Figure B

```
U P V K F W Q A X D O E R G N B L S H Y M I T C Z
A B C D E F G H I K L M N O P Q R S T U V W X Y Z
```

Figure C

```
A:  A B C D E     C:  O L M P N
    F G H I K         Y V W Z X
    L M N O P         D A B E C
    Q R S T U         T Q R U S
    V W X Y Z         I F G K H

D:  B C E A D     B:  A B C D E
    M N P L O         F G H I K
    G H K F I         L M N O P
    W X Z V Y         Q R S T U
    R S U Q T         V W X Y Z
```

EXAMPLE

Encipher with A-B plain:

```
T H E Q U I C K
R L O Y U O N P
```

Decipher with A-B as cipher:

```
R L O Y U O N P
T H E Q U I C K
```

Figure D

Arnold I. Dumey
8-280B Oradell Drive
Cranbury NJ 08512

CIPHER EQUIPMENT

TST 3336 AND TST 9761

LOUIS KRUH

The column in October 1980 in Cryptologia (Vol. 4, No. 4, pages 225-229) featured some of the products of Tele Security Timmann, Heinrich-Knote Strasse, D-8134, Pöcking, West Germany. Their extensive line of cryptographic communications systems includes a variety of devices embodying the latest state of the art technology. Two of their cipher systems not featured in the original column on TST products are described here. Note that these are two entirely different types of units designed for different types of applications.

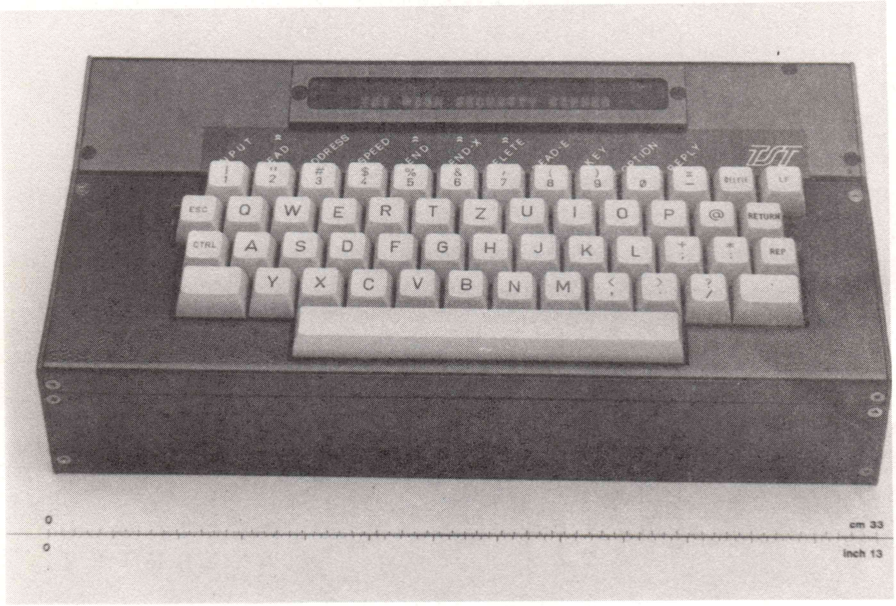


Figure 1. TST 3336 - Portable Message Transfer Set with MOT Type Cipher.

The first, the TST 3336, is a buffered on-line communication terminal with integral modem. The other, TST 9761, is Telex cipher equipment, which has no communications capabilities and operates off-line. While these two pieces of equipment are now made only on special order they represent the efforts of the company to provide secure equipmant. Readers interested in the complete and up to date line are advised to write to Tele Securiy Timmann.

The TST 3336 (Figure 1) is a portable or mobile cipher-message text transfer set with a 32 character LED-display.

The message text is first typed into the set's memory and message length can be up to 2,000 characters. Typing errors can be corrected, additional text can be appended. The available memory space is displayed upon operator command.

The message is transferred to a receiving station of the system by the operator. The transfer is by tone modulation (AFSK) so that any existing voice-grade circuit like telephone (Figure 2), UHF, VHF or HF SSB-radio link can be used.

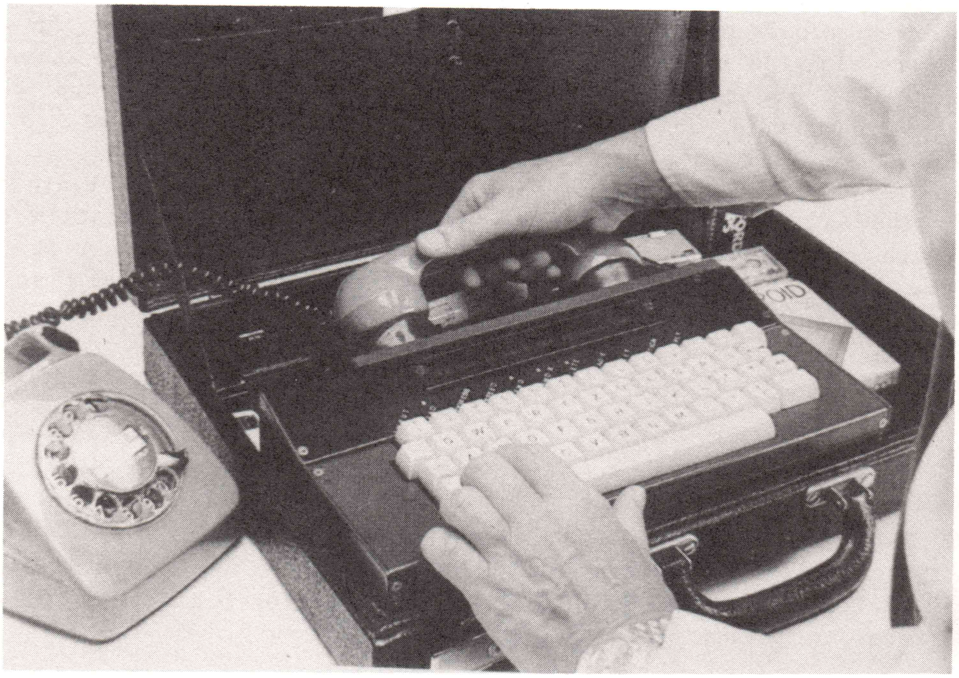


Figure 2. TST 3336 unit in an attaché case.

For direct connection TST 3336 features a 600 Ohm interface that can be adapted to all telephone and radio sets. An optional acoustic coupler permits immediate message communication from any telephone.

The speed is 65 or 32 characters per second, about 10 times faster than Telex. Each transfer is acknowledged by an automatic reply and a separate 2,000 character memory is provided for storing a received message. The message text will then be displayed automatically in rolling form and an optional printer can be connected. The TST 3336 cipher program utilizes the TST "Modified One Time Key." The key period is 10^{232}, which according to the manufacturer "is by far the absolutely highest security available, and comes extremely close to the security of One Time Key, which is by theory unbreakable."

The key, which is produced at headquarters, employing a physical noise generator, is loaded by cassette-recorder within 10 seconds. One cassette holds 180 MOT-Keys. Where keyloading by cassette is not feasible, an alternative cipher program is available with a key period of 10^{80}.

The TST 3336 is microcomputer controlled and employs C-MOS integrated circuits exclusively. When typing the message text, 6-bit ASCII characters are stored in the random access memory. During the transfer of the message, the memory contents are ciphered and formatted into a serial data stream with start, stop and check bits. The modulator changes this into audio tones and applies them to the speaker capsule, and the 600 Ohm interface adapter.

A transmit-key-relay is provided for automatic operation of a radio transmitter. The audio tones, as they are received from another station in the system, are applied to the demodulator where the digital data are recovered. These are deciphered, the clear text is stored in the receive-memory and subsequently displayed in rolling form.

A standard RS 232-C interface permits connection of a high speed printer or CRT display.

TST 9761

The TST 9761 (Figure 3) is a computer controlled automatic One Time Key Telex cipher system. As a stationary set up, it employs the TST 9000 mini-computer and a 30 char./sec. keyboard-printer with reader/perforator. A dual disk unit is used to store the operating programs and key.

The message text is first typed into the set's memory and typing errors can be corrected and additional text appended. Up to 9 messages of varying length can be stored. Total memory space is 40,000 characters with the available space printed out upon operator command. The message(s) is then ciphered and perforated on a paper tape. Similarly, a clear text paper tape can be read into the memory and then treated like a typed message.

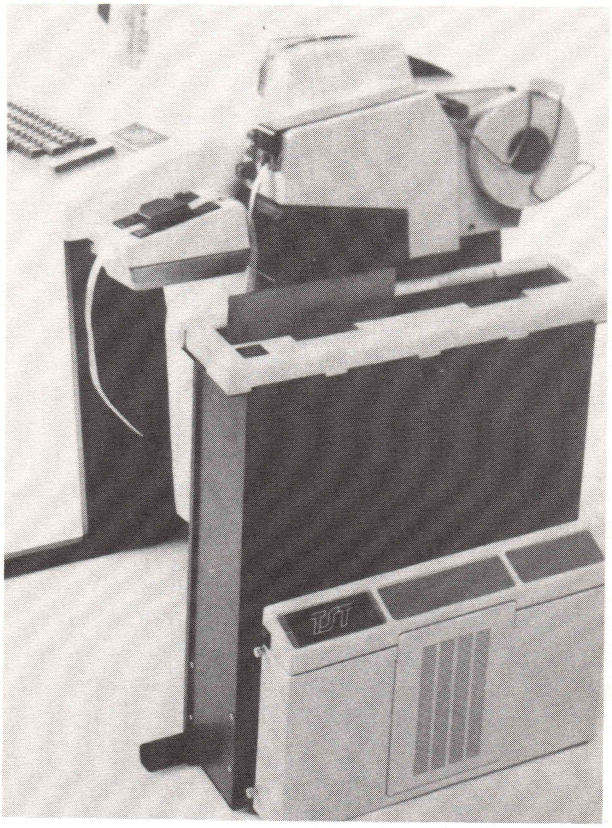


Figure 3. TST 9761 - Automatic One-Time-Key Telex Cipher System.

For maximum efficiency, a clear text perforated tape can optionally be "translated" directly into a ciphered tape. The crypto tapes are then sent via the existing public Telex network or by radio teletype. Both 5-level (CCITT No. 2) and 8-level (CCITT No. 5) tapes can be handled.

Where presently no Telex communication system exists, the optional "modem-on-line" configuration replaces the radio teletype set and the FSK keyers resp. modems. TST 9761 then presents the ciphered Telex message in tone modulated form (AFSK) directly to the existing radio transitter at 30 Char./sec., 5-times faster than regular Telex. Alternatively, a 600 Ohm line coupler or an acoustic coupler can be connected for transfer via telephone.

TST stressses that "provable absolute cipher-security can -- by theory — only be achieved with the One Time Key (OTK)" and that TST 9761 is a computer controlled OTK equipment. At headquarters, master (send) key disks are produced using a physical random noise generator (TST 0605). 512,000 key-characters are stored on one disk of 34g (1 oz), 5 times more than 1 reel of paper tape. Copies are produced for the receiving stations, one 512,000 char.-copy in 3 minutes. Only a master can be used for enciphering. One master and the required quantity of copy key-disks for deciphering are distributed to the network stations.

When enciphering, the computer will look for the marker indicating the last used key-character on the disk and start from there on to use as many as required for the message. At the end, a new marker is deposited on the disk, indicating again the last used key-character. The amount of key left unused is printed out after each encipherment. An identification number for the first key-character to be used is inserted at the beginning of the enciphered message. This number is read by at the receiving TST 9761 station, and the proper key-character is automatically read from the key-disk for deciphering. The search time for any starting point of key is less than 0.3 seconds. The automatic operation facilitates the OTK key-management and makes it secure against mishandling.

Because of the security involved with these machines, the company recommends them for embassies and military units. Also, in off-line operation there is no radiation of clear text information into the communication equipment. Computer, keyboard-printer, perforator/reader and disk unit are built for lowest on site radiation of clear text.

In modem-on-line configurations, proper shielding and pre-ciphering eliminates clear text radiation

From an electronic/construction view, the TST 9761 is composed of three separate units, connected via RS 232-C interfaces:

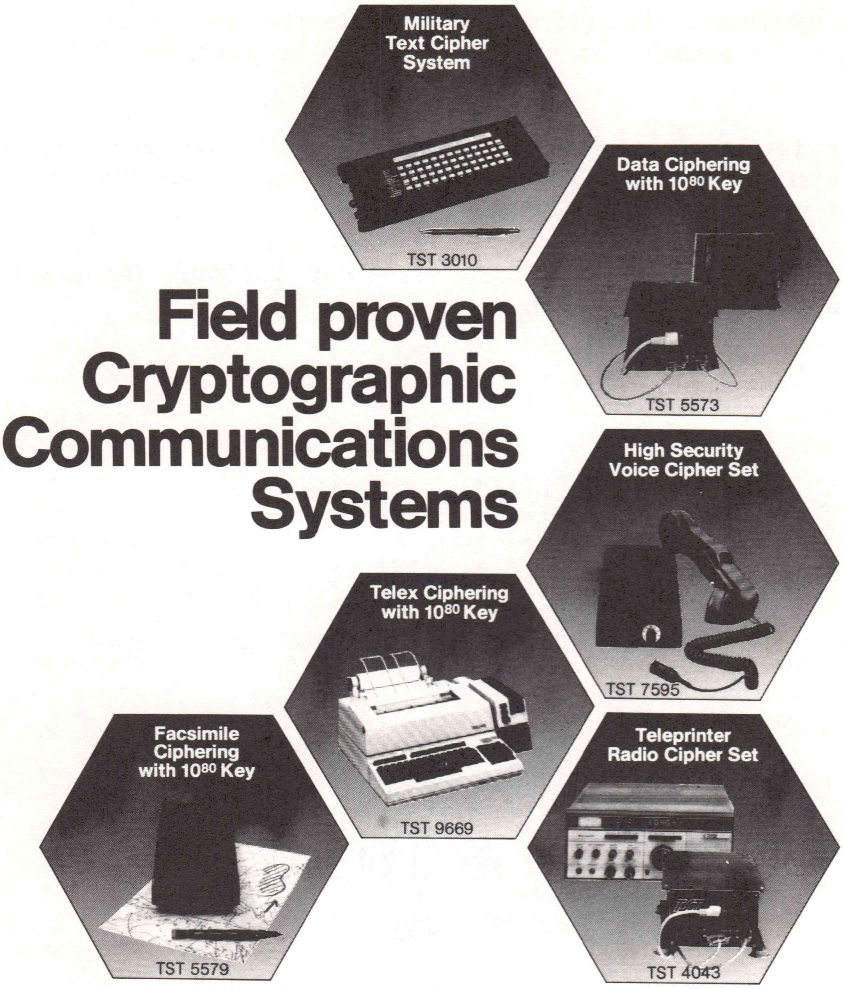
> TST 9000 minicomputer controls the operation of the cipher equipment; it retrieves/stores the operating program, the message text and the key from/on the disks.
>
> Three plug-in cards are standardly provided for the Central Processor Unit, the C-MOS memory, and the disk interface.

The keyboard-printer is a 30 char./sec. needle printer employing its own microprocessor with its own selftest function.

The reader/perforator is attached and used to read and perforate 5- to 8-level paper tape. A plunger is all that has to be changed from 5- to 8-level operation.

The reader is optoelectronic with stepping motor. Control circuitry is made up of integrated circuits, inputs and outputs are separated by opto-couplers for lowest electromagnetic radiation.

In 1980 the price of the TST 3336 was about $18,000. The price of the TST 9761 was approximately $30,000.


Military Text Cipher System
TST 3010
Data Ciphering with 10^80 Key
TST 5573
Field proven Cryptographic Communications Systems
High Security Voice Cipher Set
TST 7595
Telex Ciphering with 10^80 Key
TST 9669
Facsimile Ciphering with 10^80 Key
TST 5579
Teleprinter Radio Cipher Set
TST 4043

IACR ANNOUNCES BULLETIN BOARD SERVICE

ROBERT R. JUENEMAN

The International Association for Cryptologic Research is now operating an electronic bulletin board system dedicated to cryptography. Robert Jueneman, the Secretary/Treasurer of the IACR, is the "SYSOP," or system operator. The hours of operation are nominally from 6:30 PM to 7:30 AM Eastern time Monday through Friday, plus 24 hours on weekends.

The telephone number for the data line is 703-237-4322 (McLean, Virginia). The system will auto-answer at 300 baud or 1200 bps, using a Hayes Smartmodem 1200 which is compatible with the Bell 103 and 212A modems (but not the Racal-Vadic 1200 bps format). Almost any terminal or microcomputer equipped with a modem can be used to access the system, which runs on an IBM PC equipped with 1.1 megabytes of RAM memory and 2.3 megabytes of floppy disk memory — two DSDD and two quad disks. The system uses a public domain bulletin board program called RBBS-PC distributed by the Capital PC Users Group.

The preferred communications parameters are No parity, 8 data bits, and 1 stop bit (N-8-1) for compatibility with the XMODEM protocol for transferring binary data files, but the system will also match the Even parity, 7 data bits, 1 stop bit (E-7-1) combination. (Users who are using the popular PC-TALK.III program with 300 baud modems can also switch to 450 baud after logging on, for a 50% improvement in transfer rate. See the file TALK450.TXT after you log on.)

After dialing the telephone number and receiving the data tone or CONNECT indication from your modem, place your modem in data mode if necessary, and then send up to three Carriage Returns (sometimes called Enter) until the system responds. It will then ask you whether your terminal can display lower case characters, and proceed with a welcome message and ask you your name. Please respond with your real name, where you are calling from, and the type of system you are using. No password is required to access the board the first time, but users will be asked to enter a password to confirm their identity the next time they sign on. Since this is a serious bulletin board, hackers using pseudonyms or otherwise abusing the system will be locked out and any of their messages deleted.

Users who may be using mechanical terminals that require line feeds and/or a stream of null characters after each line can set those parameters by typing L for line feed and N for nulls the first time the menu is displayed. A special file called NEWUSERS will be displayed for first time users. Seven help files are available to assist you in using the system — you might want to save them in hard copy the first time you use them.

The bulletin board is intended to serve professionals in the field of cryptography by allowing them to post messages (which may be marked private) to each other, to distribute notices of research findings or requests for information, and upload and download files. In addition, it is intended that the BBS serve as an educational link between professionals and the general public, to let users know what cryptographic products are available and what precautions they should take to protect their information.

Manufacturers and vendors of cryptographic hardware, software, and services are invited to use the BBS to list their products. A special directory has been established for this free service. Vendors with modems are requested to upload up to 1000 words of descriptive material directly to the board, others may contact me at Computer Sciences Corp., 6565 Arlington Blvd., Falls Church, VA 22046 (703-237-2000 ext. 314). As I am planning an article which will evaluate various encryption implementations suitable for electronic mail applications, I would particularly like to hear of any DES or public key implementations in hardware or software, both for microcomputers or mainframes and especially for the IBM PC.

Although cryptography will be the primary focus of the IACR BBS, sufficient disk space is available at present to contain text files and programs for the IBM PC in several other areas as well, including communications, word processors, programming languages, graphics and utility programs, and the IBM PC DOS and hardware. No copyrighted software is available, however, and none should be uploaded, except for the various alternative distribution scheme software packages which encourage copying and distribution and request a donation if you use the package. Ways of "encrypting" or copy protecting software and ways of breaking such schemes are sometimes discussed on the BBS because of their interest to the cryptographic community, but the IACR does not condone and will not countenance the illegal copying of copyrighted software nor the unauthorized and often criminal access to other people's computer systems by so-called hackers of any age.

BIOGRAPHIES OF CONTRIBUTORS

Francis T. Guelker served in the US Signal Corps from 1941-45. He received his BS in Physics from Washington University in 1954 and his MBA from St. Louis University in 1962. He worked for Emerson Electric Co., St. Louis for 28 years retiring as Group Vice-President in 1978. He is currently self-employed as a management consultant. His interests include bookbinding, history and art, hand paper making, cryptography and travel. Address: 4052 Flora Place, St. Louis MO 63110.

Commander Robert F. Weller, United States Naval Reserve, Retired, commenced a career in Naval Cryptology in July 1944, when he was called to active duty as a Lieutenant (J.G.). Although released from active duty in August 1946, he retained his commission in the Naval Reserve and was recalled in January 1951, one of the many World War II veterans activated incident to the Korean War. He remained on active duty until 1968, serving in a variety of cryptologic operational and staff billets in Washington DC, California, and in the Pacific area, ultimately retiring with rank of Commander. In September 1969, he was employed as a civilian at the Naval Security Agency, where he performed mostly in an administrative role until May 1976, when he retired once again. Answering a special call in July 1978, Commander Weller forsook retirement and joined the team just then commencing declassification review and historical reearch functions at the Naval Security Group Command Headquarters in Washington DC. He remains engaged in that work at this time. Address: c/o Department of the Navy, Naval Security Group Command Headquarters, 3801 Nebraska Ave. NW, Washington DC 20390.

Philip M. Arnold retired in 1976 as a vice-president for research and development of Phillips Petroleum Co. after nearly 40 years with the company. As a bibliophile he collected over 2,000 volumes in the field of semeiology, sometimes known as the theory of signs, and is continuing to add to the collection, which he has given to Washington University in St. Louis MO. The collection includes such rare early works on cryptology as those of Trithemius, Silvestri, and Vigenère.

C. A. Deavours continues to offer a unique curricula in cryptology in mathematical and computer sciences aspects of the discipline at Kean College of New Jersey. In addition to teaching he is an international consultant on cryptographic matters and an excellent cryptanalyst. Address: Department of Mathematics, Kean College of New Jersey, Union NJ 07083.

Louis Kruh continues his interest in cryptology, despite the intrusion of time taken by his law school studies. His interests in cryptology span more than forty years. He collects crypto material and machines. Currently he holds the position of Advertising Manager for New York Telephone. Address: 17 Alfred Road West, Merrick NY 11566.

Donald Davies is a scientist at the UK National Physical Laboratory working on matters of data security and authentication. He began to work with digital computers in 1947, helping to build an early machine and then using it for traffic simulation and other studies. By 1965 he had moved to computer networks and developed an early packet switched network (he coined the word "packet"). Eventually this work led to a "distinguished fellowship" of the British Computer Society. Now his professional interests include the DES, public key systems and protocols for their use and his private interests include historic cipher machines. Address: Division of Information Technology and Computing, National Physical Laboratory, Teddington Middlesex TW11 0LW, England.

John DeLaurentis is a member of the technical staff in the Applied Mathematics division at Sandia National Laboratories. He received his PhD in mathematics from the Ohio State University in 1981 and spent the following year teaching at Ohio State. His interests have been primarily combinatorial probability. Address: Department of Applied Mathematics, Division 1641, Sandia National Laboratories, Albuquerque NM 87185.

John M. Carroll is a professor in the computer science department of the University of Western Ontario where he teaches computer simulation and does research on text analysis by pattern recognition. He served with the (US) Navy Security Group during World War II and Korea. Since 1968 he has worked in computer security with emphasis on data communications. His books include: Secrets of Electronic Espionage (1966), The Third Listener (1969), Confidential Information Sources (1975), and Computer Security (1977).

G. R. Blakley is Professor of Mathematics at Texas A and M University. He is the author of numerous papers in mathematics and cryptology, both of which areas have interested him for decades. Since earning the doctorate he has held teaching or research academic appointments at Cornell, Harvard, Illinois and Maryland. His research has at various times been funded by AFOSR, ARO, NBS, NSF and ONR. Address: Department of Mathematics, Texas A and M University, College Station TX 77843.

Greg Mellen is our resident expert on matters cryptologic. Although he claims not to speak algebrese, with regard to things cryptologic and mathematical he is very adept. Address: 8441 Morris Circle, Bloomington MN 55437.

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal with issue dates of January, April, July and October. The four journals issued each year constitute one volume. The January 1983 issue is Volume 7, Number 1.

Subscription prices (U.S. Dollars): $28.00 per year for U.S., $36.00 per year for non-U.S. Air Mail overseas rate is $60.00 per year. A subscription begins with the current issue as of date of receipt of request unless otherwise instructed. Back issues from January 1979, Volume 3, Number 1 to current issue are available from the Editorial Offices for $8.00 each in the U.S. and $10.00 each to non-U.S. address. Specify volume, number and issue date.

All orders, checks and inquiries should be sent to: CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803, USA. Make checks payable to CRYPTOLOGIA.

Note to subscribers: The number in the upper right corner of your address label indicates the last issue of your subscription. The right hand (single) digit indicates the Number and the remaining left hand digit(s) indicate the Volume of the last issue in your subscription. Renew your subscription now.

CALL FOR PAPERS

CRYPTOLOGIA welcomes articles on all aspects of cryptology. We especially seek articles concerning mathematics and computer related aspects of cryptology. Articles describing new cryptosystems and methods of cryptanalysis of cryptosystems, historical articles, memoirs and translations are all sought.

Send mathematical and computer related papers to Brian J. Winkel, Division of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

Send papers, inquiries and letters concerning cryptographic machines, devices and equipment to Louis Kruh, 17 Alfred Road West, Merrick, NY 11566.

Send historical and other nontechnical articles to David Kahn, 120 Wooleys Lane, Great Neck, NY 11023.

Any paper may also be sent to the Editorial Office, CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

Three copies should be submitted and one should be kept by the author as a protection against loss. Manuscripts should be legibly typewritten, or reproduced from typewritten copy and double-spaced with wide margins. All papers should have an Abstract and a Key-Word List after the title and author. Editorial style follows the University of Chicago Press Manual of Style. Please adhere to the footnoting style found in CRYPTOLOGIA articles. Diagrams should be done in black, suitable for off-set photo reproduction, and clearly labeled with a legend. Photographs should be clear and glossy. Indicate whether or not the photo print enclosed is to be returned.

While the ultimate responsibility for the accuracy of the material presented lies with the author(s), the Editorial Office will do its best through the refereeing and consultation process, to help insure correctness.

Authors will receive two copies of the issue in which their articles appear.

CRYPTOLOGIA A Quarterly Journal Devoted to All Aspects of Cryptology

Volume 8 Number 3 July 1984

Table of Contents

Published Quarterly at

Rose-Hulman Institute of Technology

Terre Haute, Indiana 47803 USA

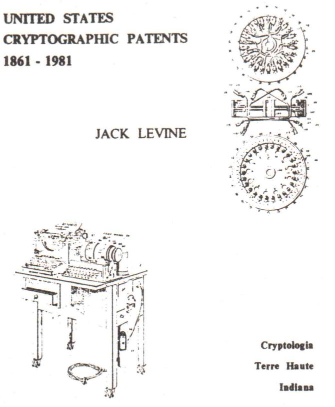
FREE FREE FREE FREE FREE FREE

STAMP COMMEMORATING ENIGMA SOLUTION

We are making two renewal offers.

We have obtained the very special First Day covers issued by Poland to commemorate the fiftieth anniversary of the solution of the German Enigma cipher machine by three young Polish mathematicians, Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski. This stamp was issued on 16 August 1983.

If you renew or extend your subscription for two years before 1 October 1984 we shall send you one of these beautiful First Day covers in your October 1984 issue. This renewal will assure that you continue to receive future exciting issues of CRYPTOLOGIA at the same subscription price for the next two more years.


UNITED STATES
CRYPTOGRAPHIC PATENTS
1861 - 1981

JACK LEVINE

Cryptologia
Terre Haute
Indiana

If you renew or extend your subscription for three years before 1 October 1984 we shall send you one of these beautiful First Day covers in your October 1984 issue and we shall send out a copy of our definitive cryptography patent book by Professor Jack Levine (while supply of book lasts). This means the current subscription rate will hold for you for the next three years in addition to getting this free reference work and the beautiful First Day cover.

UNITED STATES CRYPTOGRAPHIC PATENTS, 1861-1981, A Complete Descriptive and Illustrated List. A new book published by CRYPTOLOGIA and authored by Dr.Jack Levine, Distinguished Professor Emeritus of Mathematics, North Carolina State University.

CRYPTOLOGIA SPECIAL RENEWAL OFFER

Check your mailing label. On the right side there is a decimal number. The digit to the left of the decimal is the volume number while the digit to the right of the decimal is the issue number of the last issue in your subscription. 8.3 means that your subscription will expire with this, Volume 8, Number 3, issue. RENEW now to get a beautiful First Day cover of the Enigma Stamp and a copy of Professor Jack Levine's book, UNITED STATES CRYPTOGRAPHIC PATENTS.

_____ Yes renew (or extend) my subscription for three years and send a FREE First Day cover of the Enigma Stamp and a FREE (one only) copy of the book, UNITED STATES CRYPTOGRAPHIC PATENTS.
US - $84.00 non-US $108.00 non-US AIR MAIL $180.00

_____ Yes renew (or extend) my subscription for two years and send a FREE First Day cover of the Enigma Stamp.
US - $56.00 non-US $72.00 non-US AIR MAIL $120.00

_____ Please renew my subscription for one year.
US - $ 28.00 non-US $36.00 non-US AIR MAIL $60.00

_____ Send _____ copy(ies) of the book, UNITED STATES CRYPTOGRAPHIC PATENTS,
US - $10.00 non-US $12.00 - each - postage and handling included

_______________________ Total enclosed _________

_______________________ Insert copy of label

_______________________ or

_______________________ Write in name and address

Return this sheet with check to:

CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute IN 47803 USA

UNITED STATES CRYPTOGRAPHIC PATENT BOOK

FREE FREE FREE FREE FREE FREE